大话无线通信

丁 奇 编著



- 本书源于通信人家园09年度热帖“无线通信原理通俗解读”
- 该帖点击量突破600000次
- 本书吸收众多网友专业的意见和建议，贴近读者真实需求

人民邮电出版社
POSTS & TELECOM PRESS

大话无线通信

丁　奇　编著

人 民 邮 电 出 版 社
北　京

内 容 提 要

本书是一本介绍无线通信的通俗书，首先介绍了有线通信向无线通信的演进、通信系统的理论基础知识和无线通信的空中接口技术，然后以 GSM 系统为范例详细介绍了一个无线通信系统的组成、空中接口物理层、Um 接口的第三层协议、七号信令和通信的信令流程。

本书来源于通信人家园（http://bbs.c114.net）非常热门的技术帖“无线通信原理通俗解读”。全书采用了独特的行文风格，大量采用“水煮”的方式来帮助读者快速而轻松地对无线通信技术有一个整体的认识。本书在写法上没有采取先摆结论后进行解说的方式，而是先提出问题，再逐步给出解决问题的方法，希望读者知其然也能知其所以然，向读者揭示无线通信的奥秘。对于初学者而言，这种方式尤其有效。

本书可供无线通信技术的初学者和自学者阅读参考，也可作为无线通信从业人员的参考书。

大话无线通信

◆ 编　　著　丁　奇
　责任编辑　姚予疆
　执行编辑　刘　洋

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
　邮编　100061　　电子函件　315@ptpress.com.cn
　网址　http://www.ptpress.com.cn
　北京　　　　　　　　印刷

◆ 开本：787×1092　1/16
　印张：22.5
　字数：441 千字　　　　　　2009 年 12 月第 1 版
　印数：1 –　　000 册　　　　2009 年 12 月北京第 1 次印刷

ISBN 978-7-115-21741-7

定价：　　　元

读者服务热线：（010）67129264　印装质量热线：（010）67129223
反盗版热线：（010）67171154

前言

PREFACE



作者第一次看到近景魔术表演倒不是来自春晚的刘谦，而是来自 4 年前的一次文艺汇演。当时那位魔术师神奇得近乎诡异的手法让作者深深为之折服，于是散场之后上前想学两招。魔术师知道作者所从事的职业后掏出手机晃了晃说："这位朋友，我这个不算神奇，你这个才算神奇呢。想学魔术可以，你能教会我手机与手机之间为什么可以实现通话么？"作者一时间千头万绪，竟不知从何说起，只得作罢，不免稍感遗憾。没想到 4 年之后，又被新进公司的大学生问到了同样的问题，心中有所感触，于是开始了在通信人家园（http://bbs.c114.net）上的连载——"无线通信原理通俗解读"，尽量用诙谐生动的语言来解读无线通信，该帖反响之热烈远远超乎作者的意料，这才有了成书的想法。

的确，通信的专业知识是如此之多，作者看见放在案头几尺高的通信专业书籍都不禁乍舌。而且内容又是如此枯燥，无论是偏向基础理论层面的"信号与系统"、"通信原理"，还是偏向应用层面的"GSM 技术"、"WCDMA 技术"，要读懂都不是一件容易的事情。通信应该学什么？怎么学？对于刚刚步入通信领域的初学者而言，就像是沙漠里的一只骆驼或者是大海里的一帆孤舟，看着一望无垠的四周，眼睛里除了迷茫还是迷茫。

但凡进入一个全新的领域或者说学习一门新知识，我们要解决的都是两个问题："What——学什么？"，"How——怎么学？"。"What"从某种意义上说是属于战略范畴的东西，你得选择一个方向，然后朝这个方向一直走下去。而"How"更多的时候像是战术层面的东西，追求的是效率，怎样才能够更高效地理解我们需要学习的东西是非常重要的。

具体到学习无线通信上，我们先来回答"what"的问题。作者认为，对于刚刚接触无线通信技术的人而言，最好能够把一个实际的无线通信系统从基带到射频，从无线侧到交换侧完整通透地学习一遍，这样会对系统形成一个整体的概念，以后再遇到别的通信系统，就能举一反三，触类旁通。在本书中，作者选择的是全球使用最广泛的、最成熟的无线通信系统——GSM 系统，然后一步一步剖析这个系统，让大家来了解一个商业无线通信系统的"五脏六腑"。读透了 GSM，又何惧 TD-SCDMA、WCDMA 等技术呢？



对于“How”的问题，各人有各人不同的方法。然而实践证明，记忆一个不熟悉的东西，最快捷的方式就是将其类比为一个熟悉的东西。对于学习新知识，类比也同样是最有效的方法之一。作者在本书中采用了尽量轻松诙谐的语言和大量的类比来帮助读者迅速地建立新旧知识之间的联系。不仅如此，作者在很多章节内容的组织上，并没有采取先摆结论后进行解说的方式，而是和读者一起发现存在的问题，然后一起寻找解决的方案，力争做到让读者知其然也知其所以然。

本书共分为 8 章。第 1 章的目的是为读者提供一个快速了解无线通信的切入点。作者认为学习无线通信的最佳切入点在于比较传统有线通信与无线通信的异同，正是无线通信这些独特的地方衍生了一系列无线通信的理论和应用。第 2 章粗略地介绍了通信系统的构架，以及傅里叶变换和调制等通信基础理论知识。作者认为，只有当你知道语音信号是如何变成比特流，又是通过怎样的方式传送给对方，你才真正理解了通信的本质，才能真正体会通信的“美”，这是单纯地学习工程应用知识所体会不到的。第 3 章介绍的是 GSM 的空中接口技术。空中接口技术被称为无线通信的皇冠上的明珠，各种通信技术标准，如 GSM 和 TD-SCDMA、WCDMA，其根本差别就在空中接口上。第 4 章介绍的是 GSM 网络的组成与结构。本章对整个 GSM 网络从移动台至移动交换中心逐一进行分析，向读者介绍网络的全貌。第 5 章关注的是 GSM 空中接口物理层的设计。空中接口的频谱资源是极其有限的，为了对网络资源和频谱资源进行有效管理，GSM 网络设计了一套极为复杂的信道体系来满足实际应用的需要。第 6 章介绍的是 GSM 的第三层协议。这是一个很复杂也很让人困惑的内容，不过第三层协议在 GSM 网络里有着很重要的地位，也是无线通信技术人员必须掌握的内容。第 7 章采用了“水煮”的方式来介绍七号信令。七号信令在无线通信中有着举足轻重的地位。本章是第 8 章的必要铺垫。第 8 章的主角是 GSM 网络的信令流程。如果把第 6 章和第 7 章的内容比作单词，那么第 8 章就是要把这些单词串起来，形成一篇出色的文章，来指导 GSM 网络的工作。

读者在阅读本书的时候，可尽量沿着“总览—理论—网络—协议”的主线一直往下走，这样可以对无线通信系统形成一个整体的概念。等对整体有一个清晰的了解之后，再结合相关参考文献来了解具体的内容和细节。这样可以尽量避免“只在此山中，云深不知处”的困惑。

由于作者水平有限以及时间仓促，书中错误和不当之处在所难免，敬请广大读者和同行专家批评指正。大家可通过本书编辑的电子邮箱（liuyang@ptpress.com.cn）和我们联系交流。

作　者

致谢

Acknowledgement

在这里首先要特别感谢北京邮电大学张平教授在百忙之中抽出时间为本书作序。

感谢通信人家园（http://bbs.c114.net）的管理员以及支持我的朋友们，我从未想过一个大话无线通信的帖子能引起这样大的反响和关注。家园朋友们的支持与鼓励成了我最初写此书的动力。读书的时候，我们面对的是生涩的公式和枯燥的理论；工作的时候，我们日复一日地敲击着似曾相识的命令行，触摸着那冷冰冰的机器和板件。作为一个通信人，我们都希望通信可以生动一点，活泼一点，像邻家女孩一样，美丽又亲切；作为一个读者，我们都希望通信的殿堂，不仅有《资治通鉴》，庄严大气，处处透着理性与思辩；也希望有《明朝那些事儿》，轻松幽默，不知不觉间，轻舟已过万重山。一条新的路或许布满荆棘，或许不知所往，这让你有时候会觉得身心俱疲，有时候只感到四顾茫茫，感谢家园的朋友一路相伴，一路地出主意，我才有勇气一路走下去，为了我们共同的期望。

在这里我也要感谢中国联通益阳分公司肖智辉总经理、中国联通湖南分公司王莉经理、熊敏经理现在或曾经给予我的关心和照顾。感激在心，或无以言表，谨在此表示深深的谢意。

感谢中国联通益阳分公司蒋先遵副总经理、廖坚强经理和卜云辉助理在工作中对我的支持与指导。

感谢我的同事和朋友们帮我分担工作压力，给予我鼓励，使得我可以抽出足够的时间和精力来完成本书。

本书要献给我的母亲，多年来她一直有个愿望，那就是希望我可以成为一个作家，去那片她当知青的热土，写一写那里的山水和那个年代的生活。我来到了电信行业，而没有去学中文，成为一个笔下生花的作家，也就没有写出那样的书，不过我仍想把这本书送给她，希望她可以同样喜欢。

作　者

序

Foreword

今天，无线通信技术在深刻地影响着我们每个人的生活。随着通信技术的飞速发展和通信产业链的不断成熟，手机从最初只是高端商务群体才能拥有的奢侈品，到现在已飞入寻常百姓家，成为一种大众通信工具。无论你走到天涯海角，只要在有通信信号的地方，你都可以通过手机与他人取得联系。而随着时代的发展，手机也逐渐由一个单一的通信工具演变成一个综合的个人信息平台，财经、体育、娱乐等各种信息都可以通过手机轻松获得。

这些年无线通信行业发展迅猛，吸引了大批有志青年和年轻学子投身其中。应当注意的是，虽然无线通信业务和应用的种类繁多，但是无线通信技术本质的东西并没有发生根本的变化。就理论而言，现代通信技术依然基于香农的信息论，各种通信技术所应用的底层调制解调和编码译码等技术并没有本质的区别；就实际网络而言，无线通信系统从 2G 到 3G 依然遵循着“无线收发信机—无线收发信机控制器—移动交换中心”这样的体系架构。因此，我十分赞同作者的看法，不同无线通信技术之间并没有本质的区别，先搞明白一种无线通信技术，再去理解其他无线通信技术就会轻松很多。

应当说无线通信所涵盖的知识是比较多的，内容也较为复杂。如何快速而有效地学习这些知识是一个值得思考的问题。作者在本书中另辟蹊径，从相对简单的有线通信入手，以轻松诙谐的语言揭示无线通信与有线通信的传承与区别，为读者学习无线通信提供了一个不错的切入点。接下来全书大量采用类比的方式来讲解无线通信从空口到信令的相关技术知识，从无线侧到交换侧的相关内容。书中所举的例子生动活泼，十分便于读者理解和学习这些知识。

通信类图书通常是专业性较强，理解起来有一定难度。本书的作者别出心裁，以轻松活泼和更贴近读者的方式来阐述无线通信技术，这无疑是一次非常有益的探索。希望本书能为广大学子和从业人员学习无线通信技术知识提供一些帮助，为促进通信行业的人才培养起到一定的作用。

北京邮电大学教授、博士生导师

目录

Contents

水　煮　篇

基础理论篇

目录

Contents



目录

Contents

实 战 篇

目录

Contents



目录
Contents

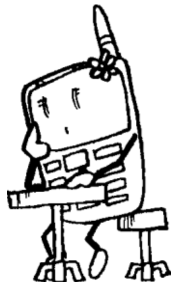
目录

Contents

水煮篇

茫茫人海，基站如何找到手机？举目四顾，手机如何找到基站？开放的无线电波，如何保障个人的通信安全？信号交叉覆盖，如何实现客户通信的完美切换？无线通信之旅，从固话开始。

第1章 Chapter 1



快速理解无线通信

1.1 引言

如同我们前言中所说的，学习新知识的最好的办法就是拿它与旧知识进行类比，认识一件不熟悉的事物最好的办法就是拿它和熟悉的事物对比。我们在本章里希望通过大量的类比来为读者提供学习无线通信的一个快速切入口，让读者对无线通信系统和运作方式有一个整体的初步认识。

1.2 空中接口和无线信道

虽然这两年手机的普及速度异常迅猛，但是提起固定电话，相信大家还是相当亲切，毕竟这是陪伴了我们十几年乃至几十年的通信工具。我们介绍手机之前先介绍固定电话，就是因为固定电话相对手机而言要简单。而且出于保护投资以及互联互通层面的考虑，无线通信的整个体系有很大部分是源于固网的，选择从固网切入便于我们学习。

无线通信和有线通信的区别，说得复杂一点，有很多很多；说得简单一点，其实只有两点：接口和信道。

首先是接口不同，固定电话的接口是钉在墙上的，插一根电话线就可以用，通过这个接口可以和固网进行联系（如图 1.1 所示）；而手机和基站通信的接口是看不见、摸不着的，我们称之为“空中接口”，手机就是通过这个空中接口和无线网络保持联络（如图 1.2 所示）。



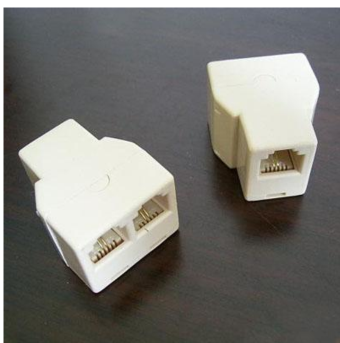


图 1.1　固定电话的接口

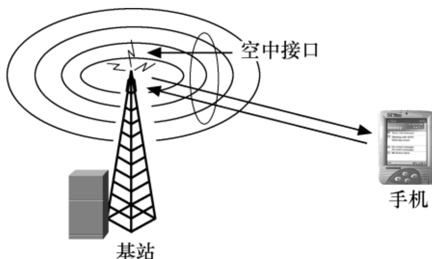


图 1.2　无线通信的空中接口

其次是信道不同，固定电话的信号是通过电话线进行传递的，称之为“有线信道”；手机的信号是通过电磁波在空中传送的，还是看不见、摸不着的，称之为“无线信道”。



图 1.3　固定电话的电话线

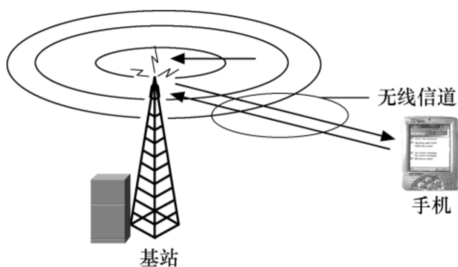


图 1.4　无线信道

可别小看了这两个名词：空中接口与无线信道，翻遍无线通信的史册，几乎没有哪一页与这两个词无关。无线通信所遇到的问题、所取得的成就，无不由这两个名词衍生而来。不夸张地说，读透了空中接口和无线信道，就读透了无线通信。

1.3　无线通信的困惑

看起来无线通信与有线通信只有两个区别：空中接口和无线信道，似乎从有线通信过渡到无线通信很简单。然而仅仅是这两个区别就让无线通信陷入了重重困惑之中。

或许有人会不以为然，不就是用空气代替铜线传递信号吗，怎么就会困惑了。那好，我们提出以下几个问题，看看无线通信比有线通信到底复杂在哪里。

问题一：一个墙上的插口通常只能对应一台电话，而基站的一面天线要同时接收很多手机的信号，如何区分哪个信号来自哪个手机？



问题二：固定电话要和网络联系是非常简单的，只需找到电话线的插口插上即可；而手机则要麻烦得多，能让它接入无线网络的基站在哪里，如何才能找到？

问题三：固定电话的位置是固定的，通信网络要找你，把信号送入指定的电话线和指定的接口即可；而无线通信就不同了，手机的位置随时在变化，谁知道手机在哪个基站下面，有电话要找你，怎么才能知道你在哪里，然后找到你呢？

问题四：在固定通信时，确定一个用户的身份是很简单的，电话线就装在你家里，想赖账，门都没有；在无线通信时代，大家都是通过电磁波在空中传送信号，没有实体接口可以确认身份，那么就得有别的办法确认你是不是合法用户，要是让非法用户进入了系统，可没法循着电磁波去找人要钱。

问题五：空中接口的电磁波是开放的，谁都可以拦截到，咱看影视剧没少看到这一幕。咱不想被人窃听，该如何加密呢？

问题六：手机在通话过程中位置会不断变化，通话环境也会随之变化，该怎样才能保证用户通话不中断呢？

1.3.1 困惑一：基站如何区分手机

我们知道，在固定电话时代，要识别一路话音信号来自哪台电话是一件很简单的事情，看看它来自墙上的哪个接口，通过哪根电话线送到电话交接箱就可以了，交接箱上的标签写得清清楚楚呢，如图 1.5 所示。

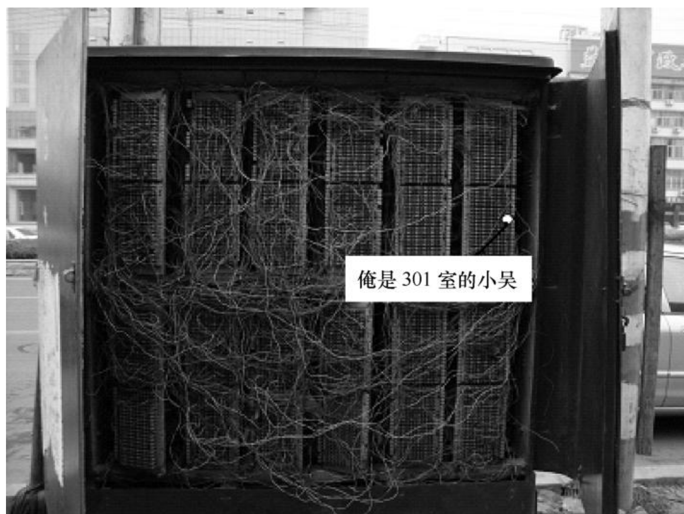


图 1.5　电话交接箱

而无线通信时代就没有这么幸运了，空中接口没有一个实实在在的插口，就是一面



天线在接收电磁波，问题是这么多手机都向天线发射电磁波，基站咋搞得清谁是谁？图 1.6 示意了这种状况。



图 1.6　谁是谁——空中接口的困惑

机器是非人类，在了解非人类的想法之前，我们不妨先了解人类世界是怎么做的。如果我们面前有好几个人在说话，我们要区分哪句话是谁讲的并不困难。那我们是如何区分的呢，物理课里有很清楚的答案，我们有 3 个参数来分辨声音——音色、音调、响度。

声波通常包含多个频率，其中频率最低的声音叫做基音，基音决定了音调。其他频率声音的强度都比基音弱，频率都是基音的整数倍，我们把它们叫做泛音，泛音和基音一起决定了音色。响度通常指声音的大小。

在无线通信网络里也照搬一下人类的区分系统，这样多省事啊。但我们很快发现，响度这个指标根本不靠谱。如果把接收信号的天线比作耳朵的话，那么响度就是指接收功率了，影响这个指标的因素实在太多了，手机离基站的远近，小尺度衰落，大尺度效应，这个“响度”一刻不停地在变化，根本不能作为区分不同手机的指标用。音色和音调也有问题，因为大家都在 20～3 400Hz 频率上说话，所以很容易产生干扰，2 个人说话分辨出来不难，8 个人说话……呃，那你的耳朵得多灵敏啊。

那么基站是如何区分不同的手机的呢。我们知道，一男一女合唱，他们的声音是很

容易分辨的，因为声波工作在不同频段，女的要高八度，而两个男的合唱则不容易区分。在这方面，手机可比人强多了，手机的滤波器对频率区分的能力远远高于人耳。所以，我们可以让手机工作在**不同的频率**上用以区分它们。另外，无线通信系统都是有自己的时间体系的，比如 GSM，在中心交换机里用晶振产生时间，然后一级一级往下传送时钟，以形成全网时间的统一，如果让手机工作在**不同的时间**里，那么也可以区分它们。

在无线通信里，对手机的区分有个术语，叫做多址或者复用，是无线通信中非常重要的概念，有关这部分的详细内容请参见第 3 章。

1.3.2　困惑二：手机如何找到基站

前面说过，对于固定电话而言，想要找到通信网络是非常简单的，只要把电话线往墙上的接口一插就搞定了。而对于手机而言，要想找到移动通信网络则要复杂得多，因为手机并不知道要建立联系的基站在哪里，这就需要建立一个机制让手机找到基站，如图 1.7 所示。

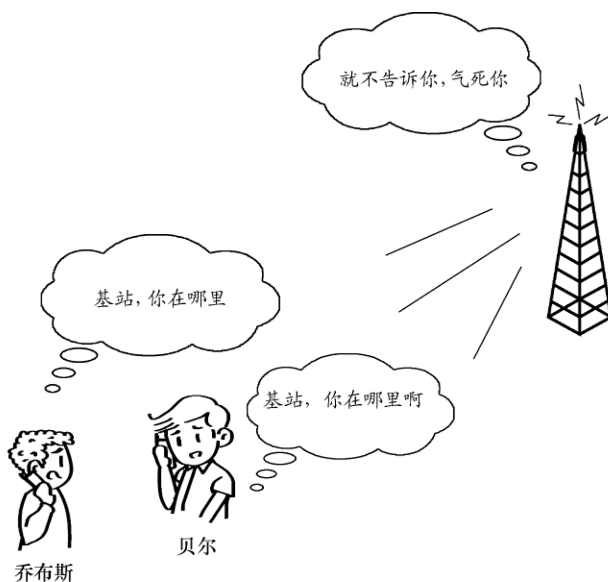


图 1.7　手机需要找到基站才能连上移动通信网络

1. 发现基站

手机到底如何找到基站？说起来与旅游团差不多，在一些非常热门的旅游景点，游客非常多，旅游团走散是再正常不过了，要靠你去找团可能有点困难。每当这时，导游总是站在高处，挥舞手中的小黄旗，用大喇叭广播着：“××地市的朋友注意了，俺在这里，俺在这里”。



基站的处理方式与此颇为类似，它总是一刻不停地向外广播信息，以方便手机找到它。然而手机又如何才能听到基站的广播信息，从而去锁定基站呢？

对于 GSM 系统而言，不同的基站广播信息时所使用的频率不同，这样 GSM 手机必须扫描整个频段，按信号的强度从最强信号开始逐一检查，直到找到合适的基站的广播信息。这很有点像我们在学校里听广播，我们拿着收音机调啊调，调到一个信号最强的台然后收听广播。不过咱们是手动挡，人家手机是自动挡。

CDMA 手机锁定基站的方式要简单得多。在 CDMA 系统里，基站固定使用一个频率（控制载频）广播信息，手机只要调谐到这个频率，就可以收到基站的指引信息，从而找到基站。系统的控制载频在整个 CDMA 通信网络中是统一的，这有点儿像无论在哪里，只要拨打 110 就可以得到警察的帮助一样，手机只要记住控制载频这个频率，接下来的事情就好办了。

2. 广播的内容

话说基站是通过广播指引信息让手机找到基站，那么基站都广播一些什么内容呢？

对于 GSM 系统而言，另外，由于手机需要调整接收频率以正确接收广播信息，那么首先需要广播频率校正信号。由于 GSM 是一个时分复用系统，时间的同步很重要，那么接下来的信息就是同步信号。

当然还会有一些其他信息，比如基站的标识、空中接口的结构参数（比如这个基站都使用了哪些频率、属于哪个位置区、手机选择该小区的优先级等）。这很好理解，就好比旅行团的导游会介绍一下当地有哪些景色、游完要花多少时间、需要多少花费等一些详细信息。你觉得合适就跟团，觉得不合适再听其他团的介绍换团也可以（根据小区的各项信息，如果当前小区不适合停留，则换到别的小区去）。

CDMA 系统与 GSM 系统类似，首先是广播导频信号和同步信号，然后再广播基站的标识和空中接口的结构参数。

3. 广播之间避免干扰

由上可知，广播信息不但帮助手机找到和锁定基站，还能为手机提供大量当前小区所必需的信息。因为我们希望广播之间不要互相干扰，不然带来很多麻烦。

GSM 相邻的基站采取不同的频率，工作的频率不同，自然不会产生干扰。就好比两个人唱歌，一个唱男低音，一个唱花腔女高音，谁也干扰不着谁。

CDMA 系统中采用的是一个固定的频率，但是扩频码不一样，也不会产生干扰。就好比一堆导游，一个说中文，一个说英文，一个说意大利语，谁也干扰不着谁。

1.3.3　困惑三：基站如何找到手机

对于固定通信而言，它知道自己的用户在哪里，因为用户的位置是固定的；而对移

动通信而言，则完全不是这么回事。手机始终处于移动状态，由于基站的覆盖范围有限，因此必然出现手机从一个基站的覆盖范围移动到另一个基站覆盖范围的情况。

尽管如此，移动网却是必须想办法找到手机，要不然就无法实现和该手机的联系，那它怎样才能找到手机呢？

一个简单的办法是通过所有的基站下发“寻人启事”，寻找该手机，这样的办法很有效，只要手机还在移动通信网的覆盖范围内，那么就一定可以找到，如图 1.8 所示。

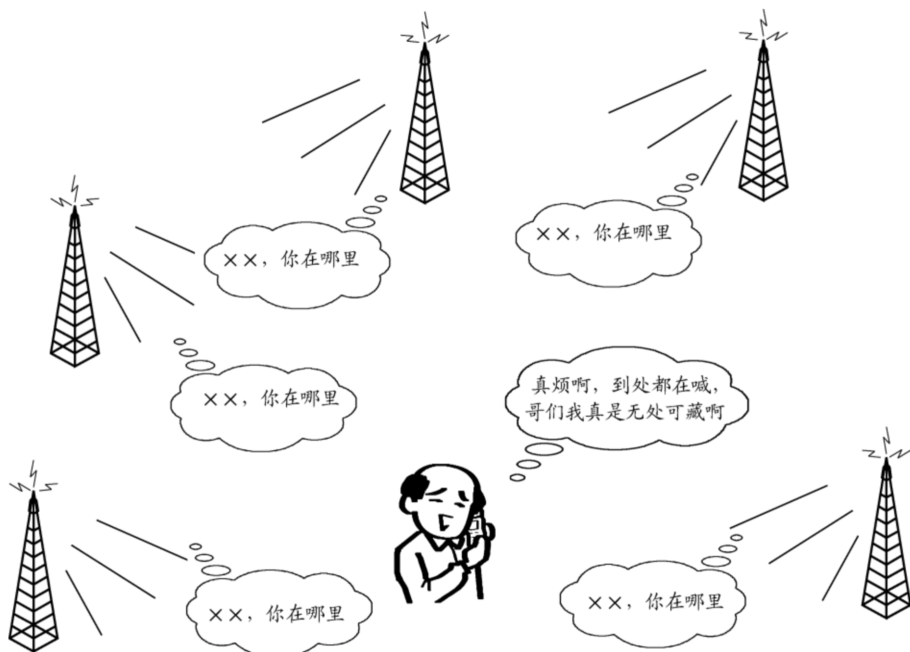


图 1.8　对手机进行全网寻找

办法虽然简单快捷，但是弊端也是显而易见的，要找一部手机居然要进行全程全网的寻找，太没效率了，我们得想想办法。想当年没有移动网的时候，我们到一个地方游玩总是用固定电话给家里打一个电话报平安：“老妈，俺在长沙开福区玩哦”，“老妈，我在北京丰台区玩哦”。万一俺当年不幸走丢了（呸，啥子假设嘛），家里人也只需要在俺走丢的区域打“寻人启事”的广告，不用在整个长沙市或者北京市打广告，这样就可以大大节省一笔广告费。

现代的无线通信系统在处理如何寻找手机这个问题上和以上方式有惊人的类似。它先是将一个城市的无线网络划成若干个位置区（类似城市的片区划分，如长沙市的开福区、岳麓区等），如图 1.9 所示。手机通过侦听广播信息得知自己所在的位置区，如果发现自己的位置区发生了变化，则主动联系无线网络，上报自己所在的位置（类似于到了



新的地方后向家里报平安，告知自己所在的位置)，如图 1.10 所示。

图 1.9　分位置区进行寻呼

无线网络收到手机发来的位置变更消息后，就把它记载在数据库里，这个数据库称为位置寄存器。等以后无线网络收到对该手机的被叫请求后，就首先查找位置寄存器，确定手机当前所处的位置区，再将被叫的请求发送到该位置区的基站，由这些基站对手机进行寻呼。

位置变更消息还有一个时效性的问题。有时候你手机所处的位置区并没有变更，但网络也无法找到你，比如你的手机电池没电了，或是 SIM 卡被拔出来了。还有一种可能是你的手机位置发生了变化，但是网络无法得知，比如说你进入了无网络覆盖的区域。在这种情况下，继续对你寻呼无疑是浪费了网络的资源。为了避免造成浪费，我们通常设定一个周期性的时间，要求手机每隔一定时间，不管位置区有没有变化，都要向网络汇报一下自己当前所在的位置区，如图 1.11 所示。对于逾时未报的，就把它当作“网络不可及”好了，直到收到它的下一次位置更新再改变状态。

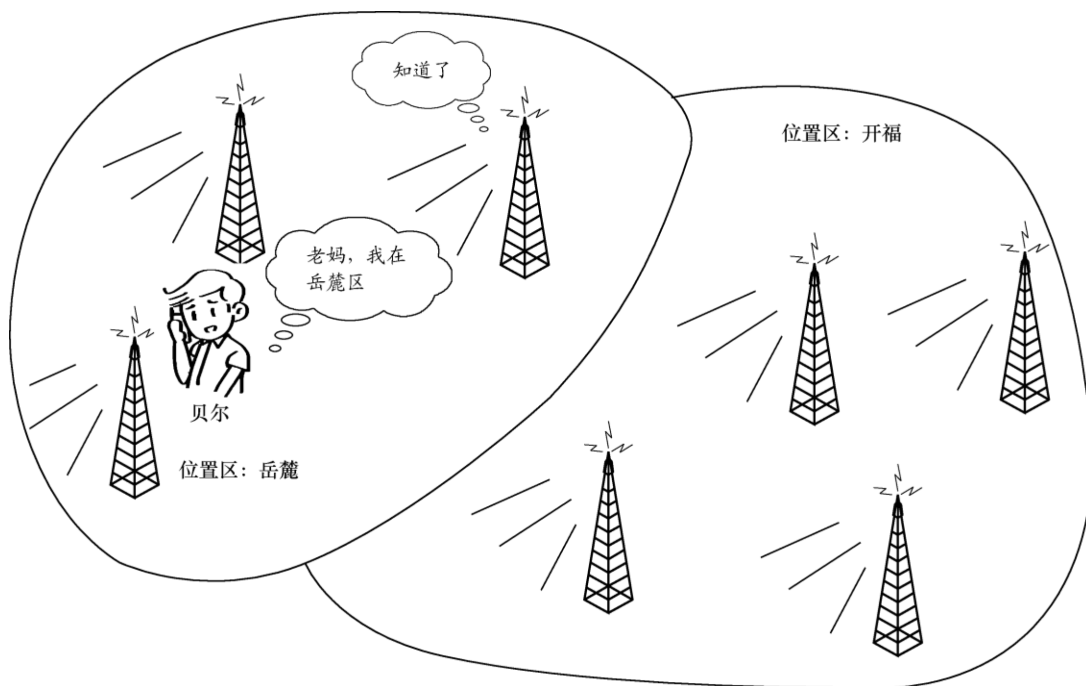


图 1.10　终端主动报告位置变更

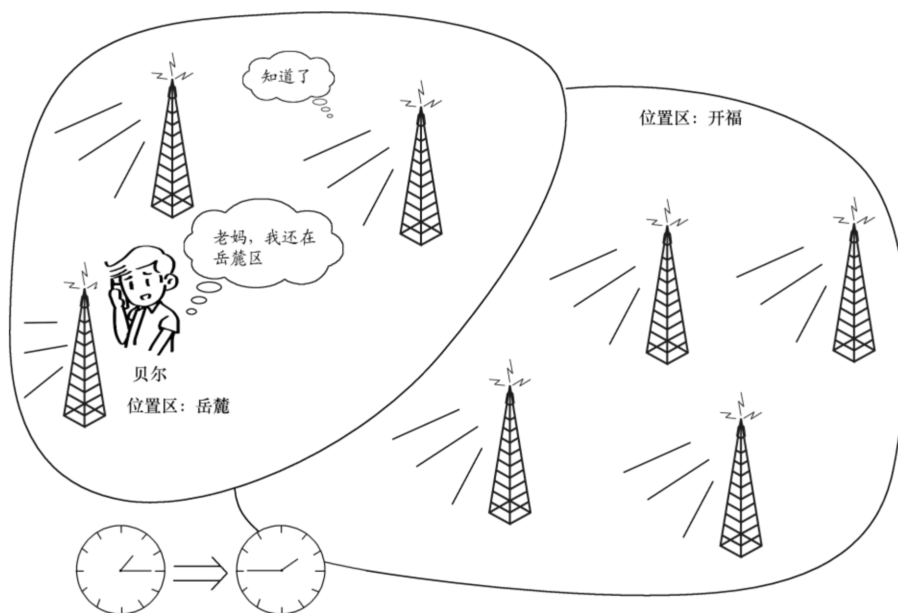


图 1.11　周期性更新（图示为 30min 后）



位置区的划分需要寻找一个平衡。划得太大了浪费寻呼资源，划得太小了手机随便一动就要上报位置区变更，同样浪费系统资源。

1.3.4　困惑四：如何识别手机用户的身份

对于通信网络而言，识别用户的身份至关重要。天底下没有免费的午餐，运营商提供的网络服务可不是免费的，收不到钱咋个养家糊口啊。

在这方面，固网有天然的优势，固网的终端一般直接接在用户家里或者公司里，跑的了和尚跑不了庙，我没有必要去确认你的身份，接口就在你家里，接口就是身份，如图 1.12 所示。



图 1.12　固定电话通过接口对用户进行识别

在移动网络里，情况就大不一样了：用户可能今天在长沙，明天在北京，没有固定的位置，系统无法根据用户的物理位置确定其身份。就好比用户可能在某公司的办公楼里用手机打电话，但这个地理位置与用户的身份识别毫无关系，你可不能去找这家公司要钱。为了保证业务的顺利开展，移动通信运营商一般每次服务前都要先确认用户的身份。

在移动通信系统中，用户是通过终端来访问网络的，因此对用户的鉴别就相当于对终端的鉴别。

在 GSM 系统中，用户的标识称为 IMSI（International Mobile Subscriber Identity，国



际移动用户识别）号。你可以把它理解为身份证号，对于整个系统而言，每个用户的 IMSI 号是唯一的，用以标识和区分用户。IMSI 号存储于 SIM 卡，SIM 卡可以独立于终端。另外，核心网络也存储了 IMSI 号，好与 SIM 卡中的信息进行比对。

CDMA 手机在国外都是机卡一体的，CDMA 系统中用户的标识是 32bit 的电子序列号（ESN，Electronic Serial Number），由终端厂商或者运营商固化在用户手机里。而在国内，为了照顾国人的消费习惯，CDMA 手机都是机卡分离的，所以它的用户标识也采取了和 GSM 相似的做法，即将 IMSI 号存储于 SIM 卡和核心网络。

问题是只有 IMSI 号是不是就足以识别一个用户了呢？实际上是不够的，这年头的假货、仿货太多了，我们得想办法防止非法用户伪造一个 IMSI 号就可以大摇大摆地在网络里横行。这就好比身份证，光靠看身份证号是不足以识别一个人的，身份证必须有防伪机制才能保证它的安全使用。

在 GSM 系统的鉴权体制里，采用的是“用户标识+密码”的方式来识别一个用户是否合法。就好比登录 Windows 系统一样，需要一个用户名和密码，有了这两个参数，用户的身份才能得到确认。

手机打电话或者上网之前，首先要向移动网络提供自己的用户标识和密码（如图 1.13 所示），移动网络收到后和数据库进行比对，如果一致，就认为你是合法用户，然后你就可以享受约定的通信服务了。

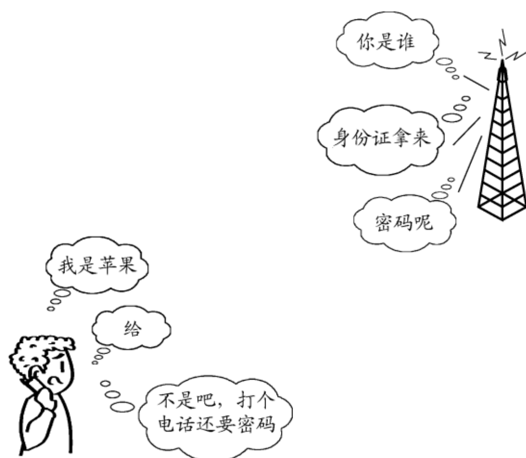


图 1.13　移动网识别用户的方式

1.3.5　困惑五：如何保证对话不被他人窃听

无线网络很令人头痛的一个事情就是要防止被人窃听，无线电波在空中是向四面八方传送的，谁都可以通过仪器在空中拦截它并窃听。在模拟通信时代，这几乎是一个无解的命题。君不见，在以前的战争年代，对阵双方的无线电通信都是能被对方截获的，所以没有人敢用明文，都只能通过密码本把它翻译成另一串字母后再发送出去。

到了大哥大时代，又不打仗，咱不能打个电话还配个机要员吧，大家都是扯着嗓子直来直去。如果附近有人架起一根天线，那可听得是清清楚楚啊。没有用过大哥大的人对此没有直观的感受，但相信不少人以前都玩过插卡的游戏机。自已在这边玩，旁边的邻居竖起天线就可以收到自已游戏的画面。

除了容量小以外，通话的安全性问题也是第一代模拟通信被人所诟病的一大问题，



所以当第二代数字移动通信系统出来以后，大哥大就迅速被取代了。

数字通信系统一个很大的好处就是可以加密，数字通信的信号是一串串比特流，比如像“01110010101010”。我完全可以拿这一串比特流和另一串特定的比特流进行与、或、非、异或等逻辑运算（可以理解为加密算法），产生一串新的数字序列。然后在接收端可以用相似的方式还原原来的信号。这样的话，即使我在空中发送的电磁信号被人家拦截到，只要他不知道我的加密算法和我加密的比特流，那他就无法还原出原来的信号。

实际上 GSM 正是这样操作的，当核心网络确认了手机的身份以后，就给手机下发一串随机的比特流（实际上不是完全随机的），手机用这串比特流与自己的密钥一起生成一串上文所述的特定比特流，然后再和要加密的用户通话数据一起通过加密算法就生成了加密信号，如图 1.14 所示。

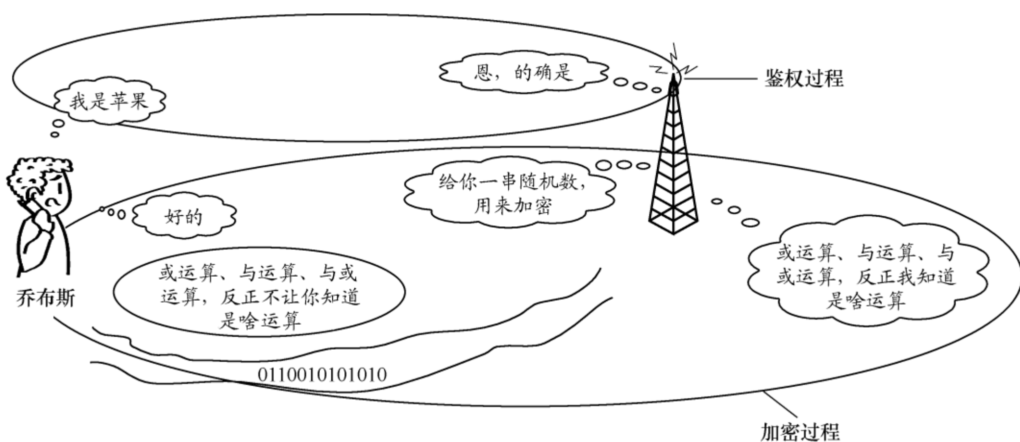


图 1.14　无线通信的加密

从上文可以知道，在空中传送的只有随机数据和加密结果，要从中推断出加密算法和加密用的密钥是非常困难的。得不到加密算法和密钥，你就无法还原别人的信号而无法实现窃听。从目前看来，数字无线通信的这种保密方式还是相当成功的。

1.3.6　困惑六：如何保证“移动”着打电话不会有问题

话说固话时代，是没有一个叫“切换”的概念。所谓固定电话，就是固定在那里不怎么动的电话。你能移动的范围是有限的，其距离取决于电话线的长度。电话粥煲得正带劲又要出门，若想边走边聊是不可能的。

这与移动通信完全不同。移动通信的特点就是用户在通话过程中位置可以不断地变动，而每个基站的覆盖范围是有限的。用户总会从一个基站覆盖的范围转移到另一个基站的覆盖范围，那么用户与一个基站的通信也不可避免地要转到另一个基站上去，这就

是“Handover”——**切换**。这个英语词汇非常形象，handover 的原意是移交。基站甲对基站乙说：“N97 这个小兄弟就要脱离我的地盘到你的地盘了，我把它移交给你了，麻烦你好好照顾它”，如图 1.15 所示。

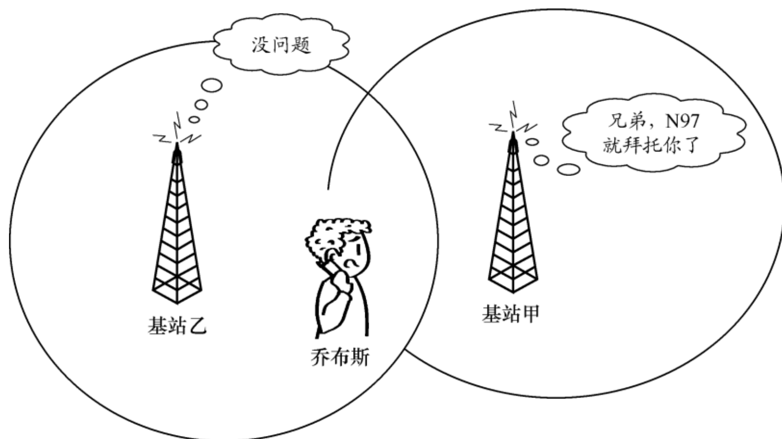


图 1.15　切换示意图

切换的方式有很多种，一种是终端首先切断与原来基站的联系，然后再接入新的基站，这种切换称之为“硬切换”，在切换的过程中通信会发生瞬时的中断。与此相对应，若终端和相邻的两个基站同时保持联系，当终端彻底进入某一个基站的覆盖区域后，才断开与另一个基站的联系，切换期间没有中断通话，称之为“软切换”或者“无缝切换”。

我们也可以拿固定电话来打个比方。固话在墙上的接口就好比无线通信的空中接口，电话都是通过接口和网络保持联系。“硬切换”就是这个固话只有一个接口和一条电话线，当你要移动到另一个房间（可以理解为另一个基站的覆盖范围），那么你就把电话线从这个房间的墙上的插口中拔出来，再插到另一个房间的插口中去，“先拔后连”，称之为硬切换。呵呵，你的固话如果要“切换”，估计也就只有这种“硬切换”法了。

对于“软切换”，我们一时间难以有清晰的理解。因为我们传统的固话都只有一根电话线和一个接口联系的。“软切换”纯粹属于无线通信的概念，电磁波的那些事儿太抽象，看不见摸不着的，难以给人直观的感受。这就需要我们有想象力，假设我们的固定电话在电话机上有两个插口，上面可以连两条电话线，在一个房间里其中一根电话线插到墙上的插口通话时，另一根电话线还可以插到隔壁的插口上实现通信，这样就可以实现“软切换”了。当你要移动到隔壁的房间咋办，不要紧，用原来就准备好了的隔壁的电话线进行通信，再把现在的这根电话线拔了，插到第 3 个房间去，这个过程不会产生通信中断，这就是“无缝切换”的由来。

对于 GSM 来说，它只有一套信号滤波器，滤波器锁定在目前通信的工作频点。而



GSM 的邻区工作频点都是不一样的，要完成切换，必须更改当前信号滤波器的频段，等调谐到要切换的频率才能和新的基站建立通信，因此必然有个先断后连的“硬切换”过程。如果一定要让 GSM 实现软切换也并非不可能，只要在终端上增加一套射频处理单元即可，这无疑会增加成本。对于 CDMA 来说，软切换要简单得多，因为它的所有载频都工作在一个频段。但当它因为系统扩容上了二载频、三载频以后，同样也会面临只能硬切换的问题。

我们在上面介绍了切换的基本概念，那么什么时候需要切换呢？

在无线通信里，通常有两个参数来衡量是否需要切换：接收信号的强度和通话质量。手机是有一定灵敏度的，信号太弱了将无法正常工作。通常信号的强度越强，通话质量就会越好。因此，信号强度是决定切换的一个很重要的指标。日常生活中，我们一般用手机信号有几格来判断接收信号的强度。

切换的时候往往会涉及多个基站，一个基站只了解自身的信号和资源情况，而并不了解其他基站的具体情况，因此通常要将终端以及基站本身测量的信号接收的强度上报给基站控制器，最后由基站控制器决定是否进行切换。

1.4 水煮GSM——无线通信系统的实现

1.3 节所述的无线通信的六大困惑其实就是无线通信与有线通信的六大区别。之所以把这些问题单独列出来，就是希望通过对比，让大家对无线通信有一个初步和整体的认识。

对概念有一个清晰的认识后，接下来的问题是如何实现它，本书从第 4 章开始，将会逐步描述无线通信实现的细节。在这里，我们不妨轻松一下，水煮一下全球最成熟的无线通信网络——GSM。

1.4.1 静静的湘水

夜，很深沉，很安静。夜幕下的湘水，静静地流淌，流往它想去的地方。河边，某集团军 A 师少将师长钟秦一个人坐在铺满鹅卵石的岸边，半闭着眼睛，似乎很享受地聆听着流水的声音。这是大战前特有的寂静，每当这时候，他都喜欢来到江边，感受流水带来的难得的宁静。

三天后就要大演习了，本次的演习地点设在湘水旁的 Y 市，由 A 师主攻，另一个甲种师主守。这次演习很特殊，为了检验部队实战的应对能力，本次演习不设导演部，不设红蓝对抗，不向作战双方公布演习的部队番号，就是为了尽最大程度模拟实战。接到



这样的任务，钟秦很是兴奋，这样的实战演习十年难得一遇啊，自然要竭尽全力去打这一仗。

然而此刻他需要宁静，A 师只是一个乙种师，装备和经费都远不如甲种师，要想赢得这样的战争，需要指挥官有一颗冷静的头脑和一双锐利的眼睛，从纷繁芜杂的一堆现象中迅速找到对手的致命弱点，一击而溃。机遇或许只有一次，把握得住才是英雄。贴近水的人，通常都会融入水的宁静，静得只听到水声和自己的心跳声，这是他喜欢水的原因，“智者乐水”何尝不是呢。

“报告，侦察营营长范胜杰汇报情况。”不知何时，范胜杰已来到身边。

“快说!”钟秦显然等待已经很久了。

“按照师长的吩咐，我们提前两个星期卧底 Y 市，得到了大量情报”。

“部队番号，对方师长姓名？”

“部队番号没有一点风声，对方的高级将领全部用汉朝将领的姓名作化名，以避免被我们查到资料，目前只知道对方师长用的代号叫‘程不识’。”范胜杰小心答道。

“没查出番号？”钟秦脸上掠过一丝不快，很快又有了笑意。“‘程不识’，知道这个也不错，起码知道了对手的大致风格。程不识在汉朝的名将里以军规严整而著称，以这个名字命名的人，治军一定非常细致严谨，这是优点，但也是我们的机会 。”

“什么机会?”范胜杰有点不解，好奇地问。

“三天后见分晓，你先去休息吧。”钟秦闭上了眼睛，陷入了沉思，范胜杰见状，知趣地退下了。

月色朦胧，如薄薄的轻纱披在人身上。湘水里月亮的倒影，随着波浪星星点点，很美。难怪《月光曲》总是那么醉人。

啪地一声立正，皮靴脚后跟相撞的声音在月空下格外响亮 ，“特务营营长上官云报到。”

钟秦喜欢这个干脆响亮的声音，面前的这个爱将做事总和他的答到一样干练。钟秦极其崇拜孙子，他尤其喜欢《孙子兵法》第十三篇《用间篇》里的一段话:“成功出于众者，先知也。先知者，不可取于鬼神，不可象于事，不可验于度，必取于人。”上官云的特务营，就是他的胜负手。

“明天两位观察员就要到了吧，来我部观摩的叫张威，去对方观摩的叫王云，对不对？”钟秦问道。

“对,”上官云答道。

“对方是个甲种师，而且据情报来看，是个高科技信息化装备的部队，我们对这样的部队的作战方式了解有限，对对方的作战风格也毫不知情，是不是？”钟秦抬起头来，看着上官云。



“的确，目前的情报对于部署作战并不够。”上官云很坦率地说出了自己的想法。

“这样的情况作战，对于我们而言，要赢可能只有一次机会。你不是克劳塞维茨的信徒吗，那么去寻找对方最薄弱的地方，倾尽全力给对方致命一击吧。对方的信息系统非常严密，侦察营无功而返，你知道该怎么做。”钟秦眼睛直视着上官云。

“这样似乎不妥吧？”上官云有点迟疑。

“兵者，诡道也，凡是演习规章里没有禁止的，那么就可以用。”钟秦不再说话，继续享受那份属于他的宁静。

上官云退下了。

1.4.2　飘荡在夜空的莫尔斯电码

清晨，王云坐着军区安排的吉普车来到了 C 师驻地——Y 市。C 师师长“程不识”早已等候在那里了。

作为一个军区参谋，王云看起来比想象中的要年轻，“程不识”过去热情地握手并说到“C 师师长常兴乐欢迎军区参谋前来观摩演习，一路辛苦了，先去军区招待所休息如何？”

王云脸上有些疲惫，目光却依然炯炯有神：“谢谢常师长，我还是想先参观一下你们的部队和信息化作战情况。信息化作战是当前的潮流，我很感兴趣。”

“那好，请随我来作战室。”常兴乐也是个爽快人。

“首先请看我们的作战电子地图，这次 C 师的作战任务是在 Y 市这个具备丘陵、平原和山地等多种地形的城市进行防御作战。我们的主要作战方针是通过暗堡串联起防线，配合野战部队进行机动作战。”常兴乐介绍。

王云不由得仔细观察起暗堡的分布来。暗堡选址均在山高险要之处或城区要害高楼，居高临下，参差有序，火力网交叉严密缝合，几无漏网之处。王云心里不由得暗暗赞叹：火力可以达到“无缝覆盖”，真将才也！

“为了让对手尽可能少地知道我 C 师的情况，C 师参谋部还针对该防御系统设计了一整套暗语和暗堡。这些暗堡，我们把它称作‘基站’，每基站可支持一个连左右的部队在附近活动作战，这些野战部队的士兵被称为‘MS’（Mobile Station，移动台）；‘基站’内有三挺重机枪呈扇形分布，构成一个火力系统，称为‘BTS’（Base Transceiver Station，基站收发信机）；暗堡之间均有壕沟或地道相通，用于传递弹药和情报，支持作战，称为‘光缆’；每几十个‘BTS’构成一个区域战斗集群，由一个‘BSC’（Base Station Controller，基站控制器）统一指挥，‘BSC’也就是团部，‘BTS’和‘BSC’合称‘BSS’（Base Station Subsystem，基站子系统）；Y 市共有 10 个‘BSC’，由一个‘MSC’（Mobile Switching Center，移动交换中心）统一指挥，也就是师部；师部



下设军情观察室，叫做‘OMC’（Operation & Maintenance Center，操作和维护中心），一刻不停地收集前方的军情。无论是 BTS、BSC 还是 MSC，我们都配备了高速计算机，用于快速处理战场复杂多变的情况，请看作战结构图（如图 1.16 所示）”常兴乐在介绍他的得意之作时，嘴角不禁浮现出一丝微笑。

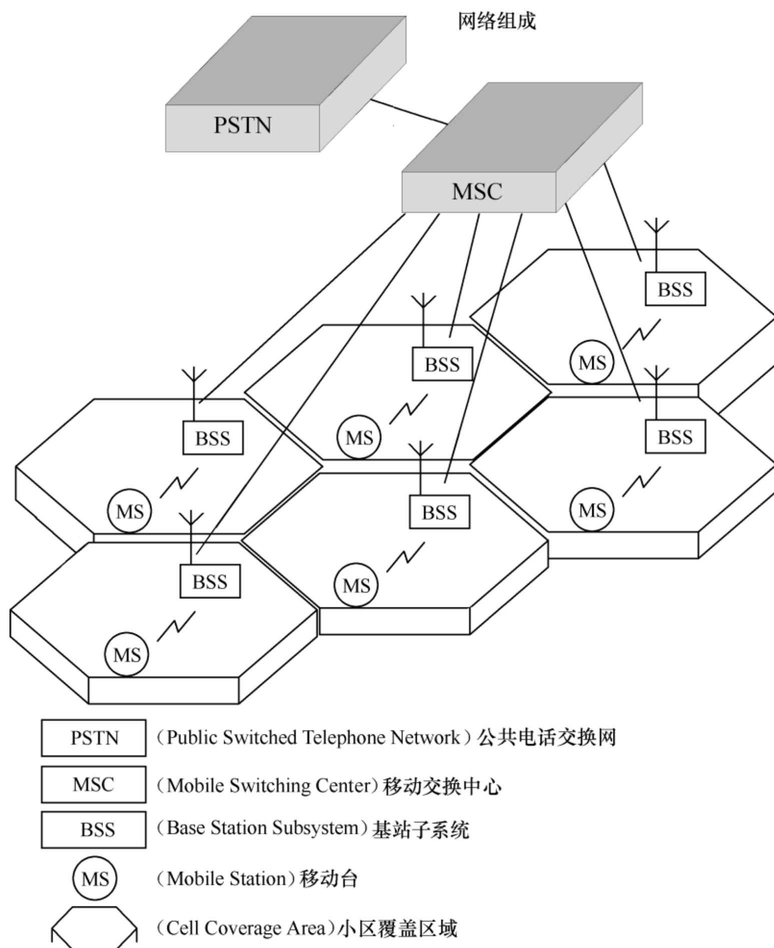


图 1.16　GSM 网络结构图

“常师长，你们的信息化作战系统那是相当的精密，但是你对整个军情的掌控都过于依赖于‘OMC’，如果对方派一支小分队化妆成你们的野战部队也就是‘MS’，对你的‘OMC’进行突袭，打掉你的信息中心，那你整个信息系统不就成了聋子瞎子了吗？”王云的眼里闪过一丝不易察觉的诡谲。

“这个请王参谋放心，跟我玩第五纵队，门都没有。”常兴乐信心满满地答道，“我们每个‘MS’野战士兵都有一个唯一识别号叫作 IMSI(International Mobile Subscriber



Identity，国际移动用户识别）等，还有一个独一无二的密码叫做 Ki 号。在军区的司令部下设了一个叫‘HLR’（Home Location Register，归属位置寄存器）的档案室，存储了这些士兵的 IMSI 号、Ki 号及其他详细信息。在师部，也有一个叫‘VLR’（Visitor Location Register，访问位置寄存器）的档案室。作战士兵的情况一旦有所变化，‘VLR’都会实时和‘HLR’联系，到 HLR 下属的特高科‘AuC’（Authentication Center，鉴权中心）里进行认证。有这个认证系统，谁想乔装成我军蒙混进来搞破坏那是不可能的。”

“哦，是这样啊。既然要做到迅速及时地识别一个士兵是不是对方乔装的，那么一定是通过无线电波进行认证咯，那么你的 IMSI 号和 Ki 号一定会在空中传送吧。电磁波是可以被拦截的，安全性问题你们考虑过没有，万一被敌方截获了怎么办？”王云继续追问道。

“呵呵，王参谋平时坐在军中大帐，运筹帷幄，决胜千里，想不到对这些技术层面的细节这样感兴趣啊。是这样的，Ki 号这个密码是不在空中传送的，我们在空中用另一串数字来代替它作为密码。”常兴乐打了个马虎眼。

“是啊，我们在空中用 Ki 号和伪随机数生成的无限不重复式密码来代替 Ki 号进行认证，想必王参谋看过《海狼行动》这部谍战片吧。片中……”C 师的一个年轻参谋讨好地补充道，结果被常兴乐盯了一眼，又把后半截话咽了回去。

“技术细节就不讨论了，我们这次演习的目的是为了检验部队在信息化条件下的各种作战方式，常师长，你们的作战方式都有哪些创新点呢？”王云饶有兴趣地说。

“我师主要的作战特点就是信息化条件下的灵活作战，又不失严谨。”常兴乐听到这个话题不由得眼前一亮，像是打开了话匣子一般滔滔不绝，“我师的作战系统十分精密而复杂，以战斗序列的作战命令而言，师部至团部的作战命令称为 MTL，军情观察室至团部的命令为 OML（Operations and Maintenance Link，操作和维护链路），团部至连队（也就是暗堡）的作战命令为 RSL（Radio Signalling Link，无线信令链路）。为了适应信息化作战的需要，这些命令都有严格的格式要求的，比如 MTL 用 C7 格式，OML 用 X.25 格式，RSL 用 LAPD 格式。”

“你们的作战命令真复杂啊！”王云不禁有点咋舌。

“这不算什么，师部、军情观察室、团部、以暗堡为基础的连部都是配备有高性能计算机的，处理这些信息不成问题。”常兴乐颇有点得意，“如今是信息化时代，对单兵以及指挥部的素质要求是越来越高了。在‘MS’野战单兵与‘BTS’的配合作战中，作战命令要更加复杂，首先我们理一下连以上建制部队的作战命令，再看看单兵的吧，请看下图（图 1.17）。”

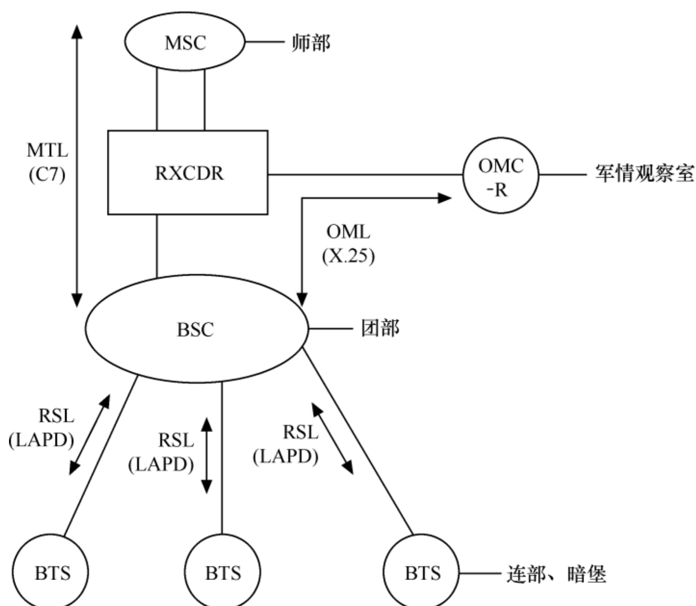


图 1.17　连以上建制作战命令一览（GSM 网络的各种协议）

“总体来说，‘BTS’暗堡指挥‘MS’单兵野战部队的作战口令相当复杂，大致可以分为 TCH（Traffic CHannel，业务信道）、BCH（Broadcast CHannel，广播信道）、CCH（Control CHannel，控制信道）等几类。”常兴乐说得口干舌燥，顿了顿，喝了口茶又开讲了，“这么多作战命令当然不是凭空产生的，都是从平时的训练和战斗演习中得来的经验。毛主席不是说我们要从战争中学习战争嘛。由于我们的步兵是在防区自由运动作战，这些口令基本是为了解决 3 类问题而设计的：①‘MS’单兵如何发现‘BTS’暗堡，以有效上报战斗情况，请求火力支援；②‘BTS’暗堡如何发现‘MS’单兵，以协同作战和避免误伤；③当‘MS’单兵运动到另一个‘BTS’暗堡火力覆盖区域时，其指挥权如何由 A 号‘BTS’转为 B 号‘BTS’，也称切换。”

王云点了点下颌，C 师治军的严谨程度有点超乎他的想象，他不由得赞许道：“常师长以‘程不识’将军的名号命名真是名副其实啊，每个细节都非常严谨。想当年匈奴犯边的时候，往往都绕开程不识的防区。”

“王参谋过奖了。”常兴乐听到这样的评价，脸上不禁露出一丝喜色，他又继续说道：“针对第一种情况，C 师对所有战斗区域编了号。‘BTS’里三面‘天线’，哦，这也是暗号，也就是三挺重机枪呈扇形分布，每挺重机枪负责的区域称为‘小区’，编号称为‘CI’（Cell Identity，小区标识）；每个‘BSC’，也就是团级战斗集群所负责的区域编号为‘LAC’（Location Area Code，位置区域码）。另外，每个‘BTS’也有一个编号，称为‘BSIC’



（Base Station Identity Code，基站标识码）。”

“BCH 口令又分为 3 种，即‘BCCH’（Broadcast Control CHannel，广播控制信道）、‘FCH’（Frequency Correction CHannel，频率校正信道）、‘SCH’（Synchronization CHannel，同步信道）。‘BTS’不断向其周围广播发送‘BCCH’口令、‘FCCH’口令、‘SCH’口令。而单兵的步话机则不断在 1 ~ 124 号频点上搜索上级发出的‘BCCH’作战口令，一旦找到该口令，也就建立了与‘BTS’的联系，也就完成了 ‘MS’单兵发现‘BTS’暗堡的过程。‘BCCH’口令主要告诉活动在周围的‘MS’单兵他们所处的团级战斗区域‘LAC’、连级战斗区域‘CI’及相邻的连级战斗区域号和本‘CI’区使用的指挥频道列表。‘FCCH’口令一旦发出，周围收到的‘MS’单兵将步话机的频率校准到相应的频道，做好战斗准备。而‘SCH’相当于‘预备’口令，要求单兵集中注意力，与‘BTS’的协同作战在时间上保持一致，另外，‘SCH’口令还把‘BSIC’告诉单兵，让他们知道自己的直接指挥上级是谁。”

王云听得津津有味，不住地点头称是。

“刚才常师长说‘BTS’暗堡是知道‘MS’单兵的位置的，这样做是为什么呢？这是如何做到的，是通过雷达吗？我很好奇。”王云略一思索，开始发问。

“这都是第二类口令的问题，我们刚刚说了，第二种战斗口令要解决的问题是‘BTS’需要知道‘MS’的战斗位置。这个非常重要，其一，我们说过，Y 市所有战斗区域都是分了区的，‘MS’在不同的区域就隶属不同的战斗集群指挥，你的位置变了，你的直接上级可能由 A 号‘BTS’转为 B 号‘BTS’，你的间接上级也可能由 C 号‘BSC’转为 D 号‘BSC’；其二，其他战斗人员要寻找你，也需要用到这个位置信息，要不就没法跟你协同作战。”常兴乐说。

“另外，‘BTS’里可是没有雷达的，一个暗堡装一个雷达，太奢侈了，也没这个必要。要知道‘MS’的位置，只能靠‘MS’主动上报，术语称为‘位置更新’，不过‘BTS’里是有高速计算机的，会把‘MS’报告给它的地址记下来，然后把这些信息逐级上报给团部‘BSC’乃至师部‘MSC’，师部会把这个单兵当前的位置在‘VLR’档案室里做个记录，这个过程很复杂吧，要不是依赖信息技术，根本不可能有这样的打法嘛。所以‘BTS’不是靠‘看’来发现终端‘MS’，而是通过记忆来‘发现’终端。”常兴乐越讲越带劲，“‘位置更新’共有 3 种情况，第 1 种情况是‘MS’单兵来‘BTS’连部报到的时候，我们这里一个调皮的参谋取了一个很奇怪的术语叫‘开机’；第 2 种情况是‘切换’，当你的位置到了另一个团部‘BSC’的控制范围时，也需要更新一下；第 3 种情况是周期性地更新，在 C 师里一般是每 30 分钟就要求‘MS’单兵上报自己的战斗位置，也就是‘LAI’号。”

王云听得很入神，手衬着下巴踱来踱去，若有所思，结果一不小心撞到了旁边一个



警卫兵，一本《诗经》从卫兵的上衣口袋里滑了出来。这本《诗经》很特别，一看就是特别定制的，它恰好跟上衣口袋一般大小。王云突然想起一句话来，心头“咯噔”了一下，脸上却平静如水。

“很经典的书嘛，可以借我读一读吗？”王云从地上拾起《诗经》，问道。

卫兵一脸尴尬，眼瞅着常兴乐，常兴乐点头默许，王云很小心地拍了拍书上的灰尘，然后把它放进了口袋里。

“今天的讲解很精彩啊，听得我都入神了。”王云说道：“常师长，今天讲了这么多，实在让我大开眼界啊，需要消化消化，今天天色已晚，别的内容我们明天继续如何？”

“哦，第 3 种战斗情况也就是切换，我还没讲完呢。”常兴乐有点愕然，“王参谋，先请休息，晚上我们聊聊天，摆摆象棋如何？”

“谢谢常师长盛情啊，我今天从军区赶来，一路实在很累了，明日再叙如何，非常抱歉。”王云有点不好意思地说。

“那好嘛，我们明天继续，今天跟王参谋一见如故啊，都有点意犹未尽。”常兴乐微笑着说。

王云面带微笑微微欠了欠身，转身往招待所走去……

大战前的夜幕，依旧寂静，月色如水，轻抚大地，好一派安详的景色。夜空，一串串莫尔斯电码如幽灵一般飘荡。

钟秦坐在河边，突然看见指挥所的探照灯朝这边发出了两长两短的灯光信号，一看腕表，刚好九点，会心地笑了，伴着月色和流水，沉思……

1.4.3 胜负手

天刚刚拂晓，钟秦及 A 师团级以上指战员已经端坐在指挥室了，还有两天演习就要开始了。钟秦眉头紧锁，在作战室里踱来踱去，不时抬起头来望着电子地图上 C 师参差有序的布防及密密麻麻火力交错的暗堡。这个“程不识”好厉害，一丝机会都没有给他。

“C 师是甲种师，装备比我们精良，机械化程度比我们高，配备了高精尖的信息设备，其作战体系也非常严谨，强攻只怕不行，只能智取。”一团团长倪星宇首先发言。

“如何智取？”钟秦锐利的目光扫过倪星宇。

“报告首长，射人先射马，擒贼先擒王。既然敌强我弱，而且敌防备严密，无懈可击，那么我们就孤注一掷，将本次作战目标直指 C 师指挥部。”倪星宇鼓起勇气提出了他大胆的想法。

“啊……”下面一片愕然，师指是防备最严密的地方，如何穿透重重防线进行斩首行



动显然是一个高难度的命题。

“好想法，不过在座的很多人不认同嘛。‘无懈可击’？什么无懈可击。备周则意殆，常见则不疑，阴在阳之内，不在阳之外。三十六计的第一计瞒天过海都忘了啊，老祖宗的智慧要牢记啊，世界上哪有无懈可击的东西。”钟秦注视着在座的高级指战员，目光坚定。

在座的都熟悉师长的脾气，知道他必定已经有了主意，于是不再说话，屏气凝神，仔细地听下文。

“‘程不识’最得意的是什么，是他严谨而精密的指挥系统，我们的突破口也恰恰就在这里。他不是觉得他的认证系统万无一失，不可能有人当第五纵队吗？那好，这就是我们想要的，他对哪方面最自信，他在哪方面的防备就会最少。我们这一次就要用一个特别小分队打掉他的指挥部。”钟秦语气铿锵有力。

“那么‘程不识’的单兵鉴权系统如何破解呢。他的每一个‘MS’单兵都是实时认证的，要蒙混过去只怕不可能。现在是信息化时代了，鉴权口令再也不像座山雕时代的‘天王盖地虎，宝塔镇河妖’那么简单。”二团团长楚天舒说道。

想起座山雕那简单的口令被杨子荣轻易攻破的情景，下面不禁一阵哄笑。

“《诗经》，没想到吧，《诗经》！上官云在提到无限不重复式密码又提到那本特别的《诗经》时，我只觉得我心里一激灵，上官云说他也有同样的感受。什么叫无限不重复式密码啊，我知道你们在座的肯定有些人对这个不了解，要不刚才回放上官云莫尔斯电报的内容时就不会不对这一细节有所反应。同志们，要加强学习啊！”钟秦语重心长地说道：“所谓无限不重复式密码，在二战时是用得相当多的。往往是双方用一本书作为密钥，然后用‘页数’、‘行数’、‘列数’来代表某个字，因为一个字可以在书中的多个地方出现，那么这个字的编码就可以不重复，所以称之为‘无限不重复’式密码。这种加密方法如果不知道密钥，要破解是非常困难的。就以这本特别的《诗经》为例，怎么对‘天王盖地虎，宝塔镇河妖’这种原始的口令进行改进呢？‘天王盖地虎’是一串随机数（RAND），假设是‘016034005006017……’，我们要根据这个随机数生成‘宝塔镇河妖’来应答，怎样生成呢？根据密钥（Ki）《诗经》来生成，我们假设生成的算法是这样的：页数+行数+列数。比如说‘宝’字出现在第 13 页第 14 行第 5 列，‘塔’字出现在第 2 页第 1 行第 7 列，‘镇’字出现在第 9 页第 17 行第 6 列……那么小兵的鉴权口令就变成‘013014005002001007……’，这个就是我们在空中要传送的应答响应了（SRES），那么原来的鉴权方根据这个应答响应一核对，正确说明是自己人，不对就给你一梭子。要命的是下次这些字又可以从不同的页数行数找，完全不重复，又是一串另外的数字。要是没有这本书，你去破解吧，啥概率分析、大数定理全部用不上，要命啊！”

“要不是上官云这次眼尖，发现了这本《诗经》，我们可能真的对‘程不识’一筹莫展了。”钟秦对自己安排的这招胜负手颇为得意。

“师长，密钥虽然已经找到。但对方生成空中比特信息序列的算法不会那么笨吧，直接用‘页数’+‘行数’+‘列数’进行编码。对方的加密算法破译了没有？”楚天舒很好奇，忍不住打岔道。

“当然破译了，我们知道原理就行了，不必理会。你还是现场检验一下破译效果吧。二团团长楚天舒，命令你带领特务营，迅速向C师腹地进行纵深穿插，目标9号高地，C师指挥部。为了避免暴露目标，命令你部徒步分散前进，明日22点在9号高地附近集结完毕。后日凌晨0：01分演习开始时向C师指挥部发动总攻，不惜一切代价端掉C师师部。上官云——‘王云’会在那里接应你们。”

“是！”楚天舒的回答很是铿锵有力，立即领命而去。一块大肥肉给了他，哪里还顾得上去研究什么破译密码。

“剩下的指战员听好了，无限不重复式密码是现代信息战的一个重要组成部分，你们就在这里给我学会，请看下图（图1.18）。”

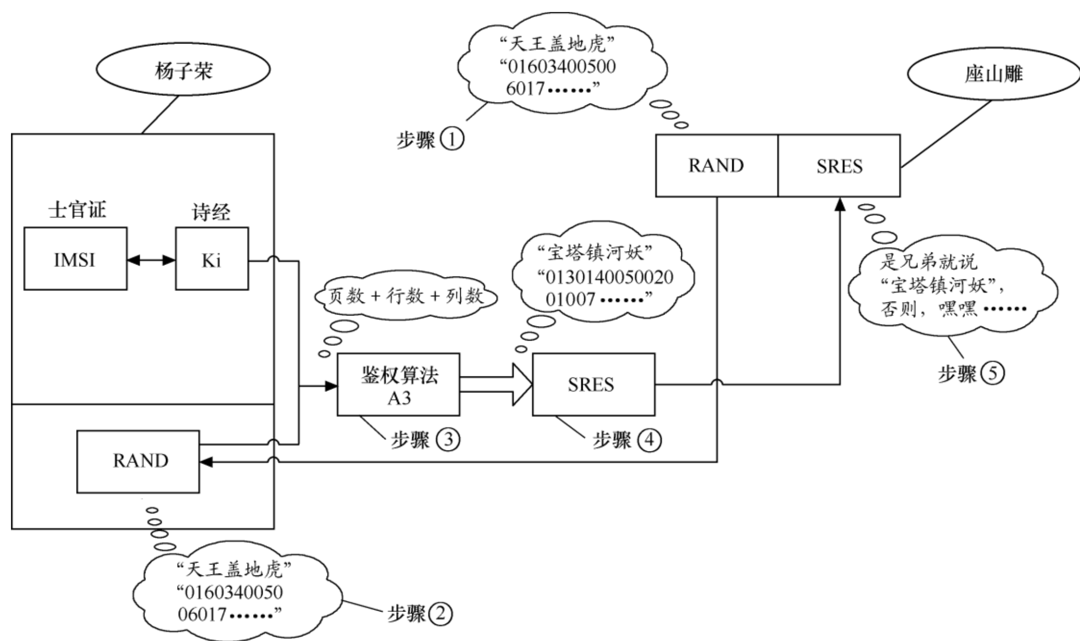


图1.18　GSM鉴权示意图

一天又十八个小时过去了，信号弹划破夜空，演习正式开始。

C师师指在后方高地上，C师做梦也想不到A师一个特务营居然能穿越重重防线来到这里，猝不及防之下被一击而溃。



一小时过去了，A 师师长钟秦赶到 9 号高地看望已经成为阶下囚的 C 师师长常兴乐，现今演习场上的冤家曾在军校一起进修过，关系还算是不错。

钟秦拍拍常兴乐的肩膀，“老同学，你处处谨慎，咋就忘记了观察员这个环节也有可能出问题呢，王云的吉普车还没到 Y 市就被我拦截了，在我那里好吃好喝都三天了。哎，这可没违反演习规则哦，不信你自己去看。”

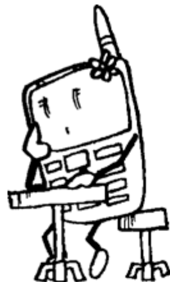
常兴乐抬起头来，眼里就写满了两字——不服。他朗声说道：“胜败乃兵家常事，不足道。一个硬币有其正反两面，新型的战法带来新的战斗力，也带来新的问题。战争波诡云谲，一时的胜负都属正常。我们之间还没完呢。”欲知后事如何，还是且听下回分解吧。

基础理论篇

举一反三，触类旁通。如何学习通信理论？不妨从日常生活中寻找它们的影子，人生处处皆学问，只要你做个有心人。

第2章

Chapter 2



通信的本质——通信系统概述

2.1 狼烟与驿站的故事——漫谈中国古代的通信

我们知道，盘古开天地之前，天地是一片混沌。然而这并不意味着1844年莫尔斯向巴尔的摩发出人类第一份电报之前，通信的世界也是一片混沌。

如果“诡辩”的话，人和人之间的对话也是无线通信。

我们把人之间的对话和现代无线通信系统进行比较，就会发现诸多相似之处。说话的人可以看作发射机，听对方说话的人可以看作接收机，人和人之间采用的语言（汉语、英语乃至法语）可以看作信源编码，承载的物理媒介都是空气……

不同的是，人和人之间传递信号是通过声波而非电磁波。声波就传递这么远，也不需要进行调制，即使你想进行调制，你的声带和喉咙也不会答应，因为它们可没这功能。

另外，人和人之间交流也很少需要信道编码，因为你一般都能听清楚对方的说话。即使偶尔你的“解码”出现问题（你没听清楚对方说话），你的大脑也比那笨笨的接收机要聪明得多，你根本不需要进行循环冗余校验（CRC，Cyclic Redundancy Check）就知道你接收的信息不完全、不充分、难以理解，然后你的大脑就丢弃这个信息包，并向发信方申请一个重传“俺没听清楚，麻烦您再说一遍”。呃，这可是收发信机在数据链路层上经典的检错和纠错机制。

如果说人和人之间的交流和现代无线通信系统存在诸多类似之处，那么我们接下来要讲的中国古代的通信系统则似乎与此不太搭界。然而既然都是通信领域的智慧，那么必有相通之处，不妨了解一二。

人和人之间的对话在日常生活和交流中显得已经足够完善了，然而人的发声系统



能发出的声波的能量是非常有限的，以至于对于稍远一点的距离就显得很无能无力。如果要进行稍微远一点的通信——比如说指挥军队战斗，那么光靠嗓子吆喝就不能解决问题了。

《孙子兵法》在第五篇《势篇》里有一句话：“孙子曰：凡制众如制寡，分数是也；斗众如斗寡，形名是也。”所谓分数，即是对部队进行整编，没有队列不成行伍。放到现代通信系统里来看，就是对一个系统里的各个单元进行编号，无论是手机终端还是收发信机，亦或中心交换机，都得编号，没有编号，一个指令下去就不知道具体找谁，也就谈不上通信。所谓形名，指的就是旗语，用旗语指挥部队变阵和进行战斗。

将士卒整编成行伍队列，以旗语指挥队伍列阵和变阵，闻鼓则进，闻金则退，这就基本组成了一支军队指挥某次战斗的相对完善的通信系统。这个通信系统相比于人和人之间的对话，有了长足的进步，无论是鼓点声。敲击金镝的声音，还是旗语，其覆盖范围显然比人和人之间的对话要大得多。

但是这个系统的缺点也是很明显的，那就是能覆盖的范围依然太有限了，一个再优秀的将领，即使在开阔的地形下，其有效指挥半径也很难超过 5 里路。这就不难理解，为什么古代大的战役几乎都发生在一个很小的区域，而不是像现代战争一样发生在一整条战线上。道理很简单，战线拉长了，指挥系统够不着啊。比如长平之战、巨鹿之战、昆阳之战，这些双方投入总兵力超过 50 万的著名战役都以某个地点命名，而到了现代，这个级别的战役往往以区域命名了，比如辽沈战役、淮海战役。

这是一定空间范围内的通信，我们可以通过鼓点和旌旗，放大声音的音量和视觉标的的大小，来延展我们的通信距离。可是对于更远的距离，比如长安和雁门，视觉和听觉都无能为力。我们在神话中构造出了“千里眼”和“顺风耳”，不过那仅仅是神话，仅仅只能代表人类的一种美好的意愿而已。

在长安和雁门这种超长距离的信息交换中，就当年而言，最要命和最要紧的信息肯定是北方游牧民族入侵的消息。为了及时传递这种信息，烽火台应运而生，通过一站一站地燃起狼烟来完成自边关向都城的信息传递，“烽火映甘泉”那是一幅怎样的景象啊。值得注意的是，烽火台和现代通信系统有一个共同的概念，那就是“中继”，光信号会随着距离而衰减，所以每隔一段距离就要建一个烽火台，重新燃起狼烟，相当于把衰减的信号重新放大一次，只有这样，入侵的信号才能从遥远的雁门传到西汉王朝的心脏——长安。电磁信号在介质中传播，无论是五类双绞线还是电缆，亦或是空气，都会有衰减和能量损失，因此隔一定的距离也同样需要中继。为什么你的网线距离不能超过 100m？因为超过 100m，信号衰减所带来的误码会使通信质量下降得令人难以接受。

就通信系统的健壮性和安全性而言，烽火台并不是百分之百值得信赖的。因为一

连串烽火台组成的是一条单链，如果其中一个点出现问题，那么整个系统的可靠性将难以得到保障。《三国演义》里关羽正是因此而丢掉的荆州，关羽水淹七军之后，兵锋直指宛、洛，为了应对徐晃带来的援军，被迫将荆州的预备队调往前线。这时候吕蒙及其士兵化妆成白衣商人，以躲雨为由进入了荆州防线的一个烽火台，手起刀落解决了守卫，结果荆州整个的预警系统就此失灵，吕蒙趁机攻占江陵，糜竺投降，关羽被迫败走麦城。

然而，烽火台并不是古代主流的远距离通信系统，虽然这种系统传播速度很快（光速是挺快的，点火也费不了多少时间）。不能成为主流的原因之一是其成本高昂（一是建设烽火台是件成本高昂的事情；二是到处找狼粪也不容易），路径固定且单一（烽火台可不是应急通信车，说开走就开走）。最要命的原因还是烽火台能够传递的信息量实在是太少了，就那么几堆狼粪，横竖排列组合就那么几种。虽然狼烟的原理和旗语颇有几分相似，但是你没法控制狼烟的运动，没法把狼烟搞得像旗语一样千变万化，那你就注定传递不了更多信息。

中国古代最主流的远距离通信系统毫无疑问是以驿站为基础的“邮局”系统，我们经常在古装影视剧中看到的所谓“八百里加急”就是这玩意儿。这个系统就是骑着马疯狂地赶路送信，遇着驿站就换马以保持行进的速度，看起来似乎没有什么可说的。值得注意的是，这么长的距离，你的信使是完全可能在半路上被劫杀的，这就引发了通信安全的问题。这个问题早在周朝就有解决方案，一为对发送信息进行加密，称为“阴符”；另一种方法和 GSM 中的跳频加密颇为相似，即将信息分为几份，通过不同的人采用不同的路径发送出去，到目的地再合为一起，就算其中一份被截，也不会泄密。以下内容来自太公姜子牙所著《六韬》一书。



《阴符第二十四》

武王问太公曰：引兵深入诸侯之地，三军猝，有缓急，或利或害。吾将以近通远，从中应外，以给三军之用。为之奈何？

太公曰：主与将，有阴符，凡八等。有大胜克敌之符，长一尺。破军杀将之符，长九寸。降城得邑之符，长八寸……

这一段就通信保密而言很经典，武王深入重地，想和大后方传递消息，就问太公咋办。姜子牙说好办啊，咱们对信源重新搞一套编码就是了，比如你杀了对方大将，就不要写“破军杀将”四个字的小纸条传给俺了，直接让信使送俺一块九寸长的木板就行了，这个加密方式只有你和俺知道，不怕泄密。

我们很快就发现，阴符和烽火台一样，面临一个致命的弱点，就是能够传递的信息量太少，或者说编码太少。阴符只能传递 8 种消息，而且很不详细，对于纷繁复杂的战



地情况而言显然是不够的。这个时候还没有发明计算机，没有二进制，没有 ASCII 编码，也没有指数和对数，想对每个汉字进行加密简直是个不可能完成的任务。聪明的周武王很快发现了阴符的弱点，他接下来就问姜子牙，俺就是一话痨，要说的话多，8 个符号不够，如之奈何？



《阴书第二十五》

武王问太公曰：引兵深入诸侯之地……其事繁多，符不能明；相去辽远，语言不通，为之奈何？

太公曰：当用书，不用符……书皆一合再离，三发而一知，此谓阴书。敌虽圣智，莫之能识。

把一封书信分成 3 份，由 3 个不同的人通过不同的路线传递，内容分离，3 个人互相不知道内情，最后传到一个将领手里，这就叫阴书。姜太公够狠的，不过没有 GSM 狠，GSM 的跳频技术是 1 秒跳 217 次。把 1 秒的内容切成 217 份，通过不同的频率发出去，这个拦截难度就大了。

古代的通信方式还有“飞鸽传书”之类，采用并不普遍，本书也就不再详加叙述。

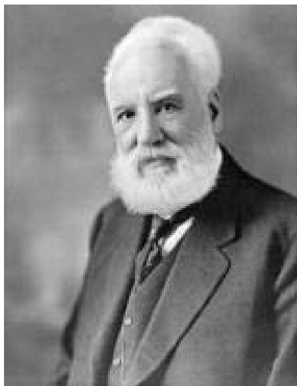
2.2 画虎画皮先画骨——通信系统构架

在 2.1 节中，我们通过对人与人之间交流机制和现代通信系统的对比，对通信系统有了一个初步的认识。在本节中，我们希望可以勾勒出一个通信系统的架构。喜欢画画的朋友知道，想要画一只老虎，先画它的骨架，骨架摸透了，画出来的老虎自是形神兼具，血肉饱满。

我们学习通信知识也是如此，先应该对整体的构架有个系统的认识，剩下的事情才是去完善细节。有了宏观的认识，微观的学习才不至于迷失方向，才不至于陷入盲人摸象的尴尬。理论往往源于对实践的归纳和提炼，因此在画出模拟或者数字系统的结构框图之前，我们不妨先了解一下贝尔和他的电话。

2.2.1 电话之父——贝尔

通信经历了一个从模拟通信到数字通信的发展过程，说起模拟通信，就不能不先提到贝尔（图 2.1 所示）。亚历山大·格雷厄姆·贝尔是公认的电话之父，以他的名字命名的贝尔实验室更是因为一直引领通信潮流而享誉世界。值得注意的是，贝尔原来是一个语音专业的教授，对发声原理有着深刻的认识，这对他后来发明电话或许不无裨益。有


图 2.1 贝尔

趣的是，发明电报的莫尔斯也非电磁专业的科班出身。莫尔斯 41 岁时还只是一个画家，他有一次在大西洋中航行的一艘邮船上，听到另一个在电磁学领域同样不靠谱的美国医生杰克逊给旅客们激情澎湃地讲解电磁铁原理，由此激发了他用电磁波传递信号的梦想。

12 年后的 1844 年，莫尔斯电报在华盛顿国会大厦联邦最高法院会议厅诞生。俺的神啊，真是有梦想谁都了不起，这个世界太疯狂了！

牛顿说过，他能取得这么多成就是因为他站在巨人的肩膀人。贝尔同样如此，在他之前，欧洲已经有很多人在进行这方面的设想和研究。早在 1854 年，电话原理就已由法国人鲍萨尔设想出来了，6 年之后德国人赖伊斯又重复了这个设想。原理是：将两块薄金属片用电线相连，一方发出声音时，金属片振动，变成电，传给对方。但这仅仅是一种设想，问题是如何构造送话器和受话器，怎样才能把声音这种机械能转换成电能，并进行传送。

贝尔遇到的第一个挑战——怎样把声波转化为电信号？

最初，贝尔试图用电磁开关来形成一开一闭的脉冲信号，但是我们知道，声波的主要频率分布于 20～3 400Hz，对于这样高的频率，企图用机械式的电磁开关来实现信号的转换显然是行不通的。道理不难理解，凡是机械运动必有惯性，要改变物体的运动方向或运动方式必定需要时间，要设计一个每秒以非均匀方式“开—关—开”3 400 次的机械开关，未免太骇人听闻了。

最后的成功源于一个偶然的发现，1875 年 6 月 2 日，在一次试验中，他把金属片连接在电磁开关上，没想到在这种状态下，声音奇妙地变成了电流。分析原理，原来是金属片因声音而振动，在其相连的电磁开关线圈中感生了电流。

图 2.2 就是 1876 年贝尔发明的电话机核心部分的素描简图，椭圆形圆圈所示的部分即电磁信号与声波信号的转换部分，我们可以清晰地看到那片薄薄的金属片。

这个电话显然与我们脑海中对固定电话的印象大相径庭，图 2.2 中所示的部分既没有送话器（话筒）也没有受话器（听筒），这怎么打电话啊。

其实贝尔的设计中是有听筒和话筒的，要不然也不能将其称为电话了。不过样子委实怪异（如图 2.3 所示），您肯定认不出它是电话来，您非要说它是广播，那俺也没办法，谁让它弄了个那么大的话筒呢。

贝尔发明了电话，另一位大发明家爱迪生也没有闲着。1876 年爱迪生发明了炭精式送话器，也获得了发明专利权。炭精式送话器比贝尔永磁式送话器更灵敏。故现代的电话机（如图 2.4 所示），基本上是爱迪生送话器与贝尔受话器的结合。



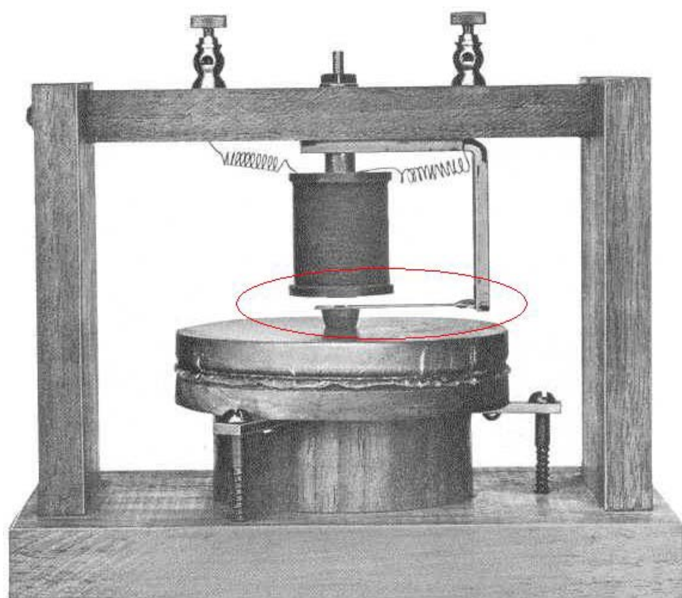


图 2.2　1876 年贝尔发明的电话机的核心部分

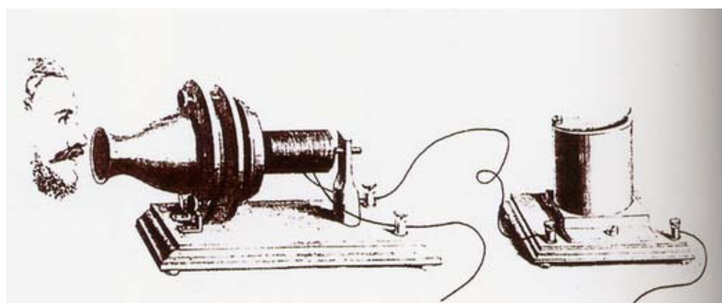


图 2.3　贝尔的第一架电话



图 2.4　现代电话

我们在探讨贝尔电话的时候并没有提到调制，也并没有提到多路电话之间的交换，而这恰恰是现代通信系统中非常重要的环节。之所以不涉及这部分内容，是因为贝尔发明的电话最初用于的是点对点的专线通信，距离也并不长，既不需要调制也不需要进行程控交换，所以我们把这部分内容放到后面的环节来阐述。

2.2.2　模拟通信系统架构

这一节我们希望能从贝尔电话这个具体案例中提炼出更具有一般性的东西，这比生硬地先给出一个框图或许更容易理解。我们把具有连续的随时间变化的波形信号称为模拟信号，语音信号是个典型的模拟信号。通常情况下，影像信号也是模拟信号，

当你举起摄像机进行摄影时，通过凹凸镜成像的光学信号的变化当然也是连续的和随着时间变化的。

无论是哪种模拟信号，无论你是声波也好光学信号也罢，如果你想把它从一个城市实时地传送到另一个城市，你几乎无可避免地都会遭遇“**贝尔挑战**”，即如何把它转变为对应的电信号。

你或许在老师指导的物理课上自制过“电话”，说话的双方各拿一个纸杯既充当听筒又充当话筒，杯底打一个小洞用于系棉线，这根棉线就充当电话线了。把棉线拉得直直的，这两个纸杯还真能凑合当小电话用。

理论源自生活固然不错，如果你凭此就认为声波信号或者光影信号可以直接用于通信，电话可以改名为“声话”或者“光话”的话，那么贝尔估计会气得从地底爬起来，拉上哆啦 A 梦用时光机把你拖到 1876 年，让你整个“光话”给他用用。

至少人类到目前为止依然没有跳出贝尔的窠臼，遇到任何信号，只要是打算用通信系统将其发送出去并在接收端有效还原为原来的信号，那么第一个遇到的问题依然是——“**如何将它转化为电信号？**”

讲到这里，我们渐渐对模拟通信系统的构架有了一个比较清晰的概念。在这样一个系统里，我们首先需要一个输入信号变换器，将模拟信号转换为电信号，就如电话的话筒一样，话筒把语音信号转换为电流信号；通过中间的信道（比如电话线）传输到接收端，又需要把电信号转化为模拟信号，以便于人理解，就如电话的听筒一样，听筒把电磁信号转变为声波信号，因此我们在接收端还需要一个变换器。

由此，我们可以勾勒出一个模拟通信系统的基本框架，如图 2.5 所示。

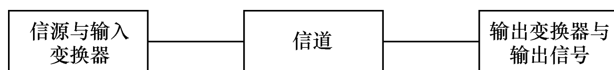


图 2.5　模拟通信系统功能框图（不含调制解调）

图 2.5 所示的模型源于贝尔电话的雏形，并没有考虑到调制，实际上，低频信号并不利于传输，需要将其调制到高频信号上去。具体的原因我们在后面的章节中再进行详细叙述，我们将图 2.5 修正为如图 2.6 所示。

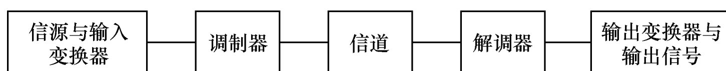


图 2.6　模拟通信系统功能框图（含调制解调）

图 2.6 也还并不是一个完整的通信系统构架图，因为没有考虑到信道乃至发射机接收机本身产生的噪声。噪声是一个通信系统不得不考虑的因素。噪声与通信系统如影随



行，虽然很令人讨厌，但是却不得不接受它的存在。我们把噪声这个因素考虑进来，就形成了一个相对完整的通信系统构架，如图 2.7 所示。

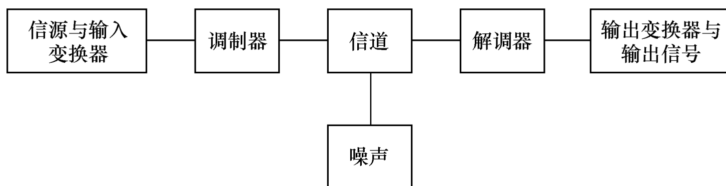


图 2.7　模拟通信系统功能框图

2.2.3　数字通信系统架构

模拟信源的输出还可以转化为数字形式，消息可以通过数字调制后发送，并在接收端解调成数字信号，然后对数字信号进行译码，还原成模拟信号。数字通信系统相对模拟通信系统，无非是在发送端和接收端都增加了一个“模拟—数字”转换模块。这个模块在日常的数码产品中很难用肉眼看到，不像进行“声—电”转换的话筒和听筒那样能给人留下直观的印象。

幸运的是，有一种家电的“模拟—数字”转换模块是独立的，那就是数字机顶盒（如图 2.8 所示）。我们原来的电视都是模拟电视，广电在闭路有线电视线上传输的也是模拟信号，现在正大力推广数字电视，而我们的电视终端却不能直接支持数字信号，所以不得不再在电视上叠加一个数字机顶盒，完成从模拟信号到数字信号的转化。其实在中国，最初推广数字机顶盒的并非是广电而是盛大网络，陈天桥与唐骏当年推出了雄心勃勃的“盛大盒子”计划，然而其产品后来却没有能够得到消费者的认可，最终成为了一堆泡影。



图 2.8　数字机顶盒

综上所述，我们给模拟通信系统增加一个“模拟—数字”转换模块，也就是俗称的“编码模块”，这成了数字通信系统的雏形，如图 2.9 所示。

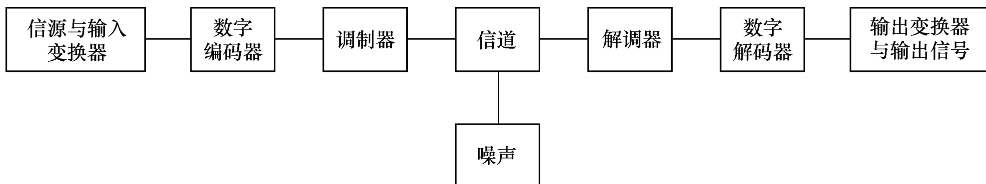


图 2.9　数字通信系统初步功能框图

在数字编码器这个功能模块上，有很多东西其实颇值得玩味。我们希望编码尽量简洁，不要啰唆，尽量减少冗余信息，对这一块内容的研究，我们称之为信源编码。然后，我们发出去的编码一路上会受到噪声的干扰，也许会丢失不少信息。到了目的地后，我们希望接收端可以根据编码所包含的一些内容，对信息的完整性作出一个判断，尽量恢复还原原来的信息，对这一块内容的探讨，我们称之为信道编码。我们就这样把数字编码器拆成了信源编码和信道编码两个功能模块，于是对图 2.9 再进行修正，如图 2.10 所示。

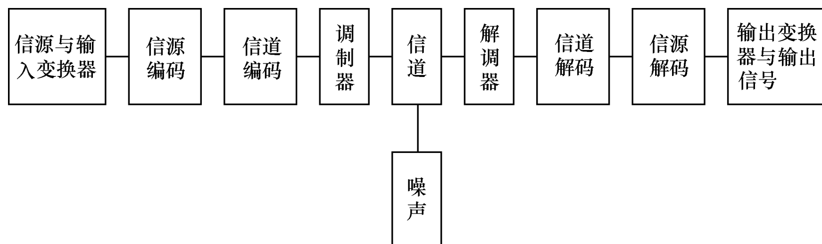


图 2.10　数字通信系统功能框图

调制、信源编码和信道编码都是数字通信中非常重要的概念，在这里，我们只是一笔带过，详细的内容留待后面讨论。

2.2.4　数字通信为何独领风骚

读书的时候，老师的一句话让我印象非常深刻："通信的世界，过去是属于模拟的，现在和将来是属于数字的，但未来的未来必定还将是属于模拟的"。

这番话或许不无道理，因为我们知道，模拟信号变为数字信号，第一个关键步骤在于采样。奈奎斯特定理已经证明了当采样频率大于两倍带限信号带宽时，信号可以完全由其采样样本来恢复。然而我们知道，冲激采样在物理上是不可实现的，即使是零阶保持采样也不可能真正实现，因此在采样环节上不可避免地存在失真。其次，采样之后得到的电平值，还必须经过量化，数字通信系统是无法处理无限多个电平值的，必须要将其按区间划分，变成有限多个电平值，才能转变为数字。在量化这个环节，也同样不可避免地存在失真。

实际上，在我们的生活中，也的确存在模拟通信系统优于数字通信系统的情况。比如说，电影一般而言是采用胶片拍摄的，胶片能够更加细腻地体现场景的细节和氛围，在色彩、光线变化、影调等各个方面都比数码能包容的程度更高。光学摄像机就是典型的模拟通信系统，它的原理是通过凸透镜将光信号在胶片上成像，优质胶片的成像质量目前还是优于数码产品的，只是它们的价格十分高昂。

然而在现代社会中，数字技术的应用却远远超过了模拟技术。大哥大被小巧的 GSM



手机踢进了博物馆，磁带被 CD 扔进了垃圾堆，就连模拟电视也即将被数字电视所取代。我们不禁要问，数字通信系统到底有什么好，为何俨然有一统江湖之势？

数字通信相对于模拟通信，其最大的一个优点在于对噪声的处理。信道噪声或者干扰造成的差错，原则上都是可以通过差错编码加以控制的。

数字通信的这个优点在长距离通信时显得尤其重要。数字传输允许对数字信号进行再生处理，这样就可以在每个再生节点消除噪声的影响（如图 2.11 所示）。而与此相反，长距离传输中叠加到模拟信号上的噪声会随着模拟信号电平的周期性放大而逐次累积（如图 2.12 所示）。

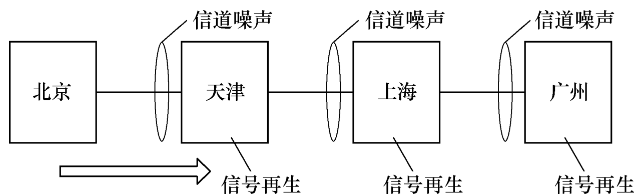


图 2.11　数字信号的消噪处理

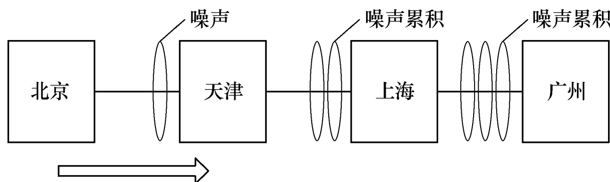


图 2.12　模拟信号噪声的累积

数字系统的另一大优点是便于保密，我们可以对基带信号进行人为的扰乱以实现加密。比如说面对“00110100110001”这么一长串二进制比特，我们可以对其加上一串伪随机序列“01011100101001”。如果第三方要知道原来的信息，他就必须知道所采用的算法和伪随机序列，这个难度是很大的。当然我们这里的加密算法仅仅是一个二进制加法，未免显得过于简单，实际应用中的加密算法比这个要复杂得多。

数字系统还有一个优点就是实现的成本比较低，成本就是竞争力嘛！

2.3　信号的基础知识

2.3.1　信号的概念——从狼烟到电磁波

几乎所有与通信有关的教材类书籍的开篇都是讲“信号”。如果不是，那么一定会在前言里注明——“本书的读者应当具备‘信号与系统’的相关知识”。以“信号”作为通

信最基础的知识是很自然的，信号承载了人们所要传递的信息，可谓“无信号，不系统”，如果都没有信号要传递，那么现代的各种通信系统也就失去它的意义了。

那么什么是信号？什么是系统？很简单，通信系统承载的信息流就是信号。“鸿雁传书”，鸽子腿上绑着的情书就是信号，这识路的鸽子就是这对情侣的通信系统；“烽火连三月”，烽火台上燃起的狼烟所代表的入侵信息就是信号，这一站接一站的烽火台就是古代特殊的战争通信系统。

作者不是历史研究者，既无意去八卦周幽王烽火戏诸侯的轶事，也无意去探究一个驿站（古代的官方邮局）的下岗职工李自成是如何大变活人成为闯王的。念叨这些陈年往事只不过想和读者说明，所谓的信号与系统既不神秘也不新鲜，莫尔斯发明电报、贝尔发明电话之前，通信系统（八百里加急）乃至无线通信系统（烽火狼烟）照样存在。现代通信系统如此迅速地发展应当归功于电磁波的传播速度，光速的魅力让其他通信系统相形见绌，也最大程度地满足了人们对于沟通实时性的要求。

下面就回到本节的正题——电磁信号。电磁信号是一个时间的函数，这很好理解，不同的时间里它都有不同的值。同时，电磁信号还可以表示为频率的函数。也就是说，一个信号是由不同的频率成分组成的，这个观点并不好理解，因为我们的日常生活中通常都是以时间的观点来解读信号的。古有沙漏、日晷，今有手机、手表，无论是二十四节气表还是列车时刻表，都说明了人们已经习惯用时间来衡量与标记这个世界。如果谁想用频率来作为刻度，那简直就和用二进制来做加法一样显得有点奇怪。

然而，从频域的观点来理解信号对于一个从事通信技术工作的人来说又是如此重要，以至于缺乏这种意识就寸步难行。从奈奎斯特采样定理到香农理论，从GSM到WCDMA，通信的每一寸土地每一个角落都渗透着频率的思想，它如氧气一般，无处不在，且不可或缺！

其实我们的日常生活中对于频率也不是完全没有直观的认识。相信大家都看过男女声合唱，一般都是一唱一和，一个高八度一个低八度，音乐比这个世界上的任何东西都更讲究和谐与优美，这或许也是它如此受大众欢迎的原因吧。在这里，这个所谓的高八度与低八度指的就是声带的振动频率。

2.3.2 信号的时域概念

现在我们就以时域的观点和频域的观点来对信号做一番介绍，这或许会要用到一点数学知识，还好这并不困难。

从时间函数的观念来看，一个信号或者是模拟的或者是数字的。如果一段时间内，信号的强度变化是平滑的，没有中断或者不连续，那么这种信号就称为模拟信号（analog signal）。如果一个信号在某一段时间内信号强度保持某个常量值，然后在下一时段又变



化为另一个常量值，这种信号就称为数字信号（digital signal）。模拟信号和数字信号的区别可以很容易地从图形上看出来，图 2.13 所示为这两种信号的例子。这里的模拟信号可能代表了一段噪声，而数字信号则代表了二进制的 0 和 1。

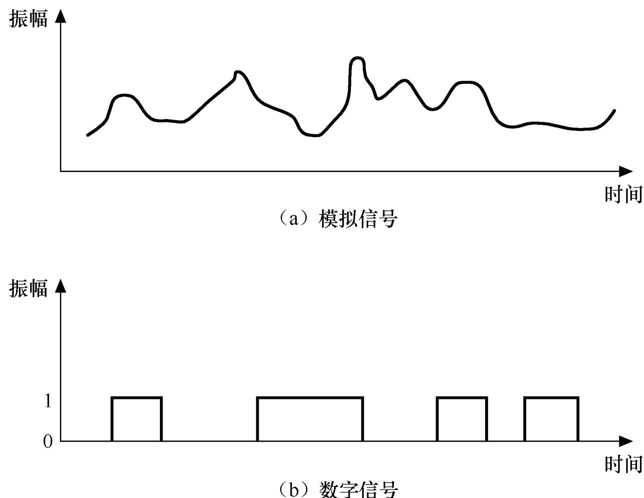


图 2.13　模拟信号和数字信号波形

最为简单的信号当然是周期信号。何谓周期信号？周而复始不断重复的信号就叫周期信号。比如我们说“做一天和尚撞一天钟”，和尚撞钟念佛，天天如此，你也不妨把它理解为周期信号。周期信号为啥简单啊，每天一样能不简单么，柿子总要挑软的捏，我们对信号进行分析，也往往从周期信号开始。

也可以从数学上来理解周期信号，当且仅当信号 $s(t+\mathrm{T})=s(t)$时，信号 $s(t)$才是周期信号，这里的常量 T 是信号周期。如果不满足这个等式，那么信号就是非周期的。

图 2.14 示出了两个典型的周期信号，一个为正弦波，一个为方波。

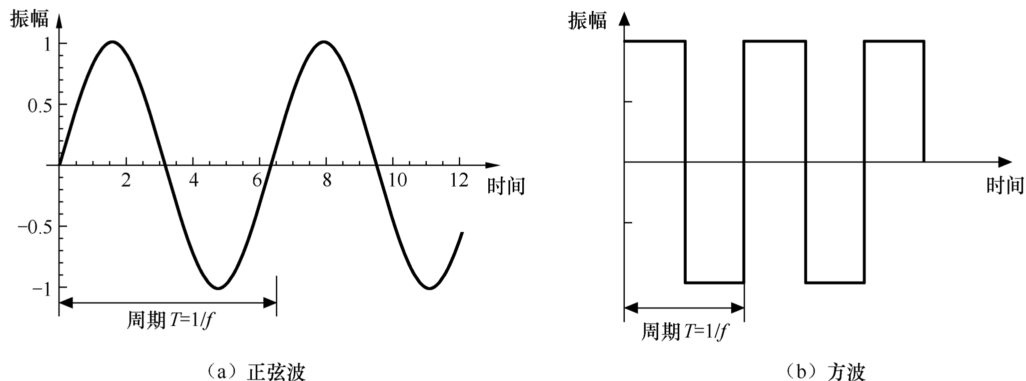


图 2.14　周期信号示例

正弦波是最基本的模拟周期信号，简单正弦波可以用以下 3 个参数表示：幅度（A）、频率（f）和相位（θ）。振幅（amplitude）是指一段时间内信号的最大值。频率（frequency）是指信号循环的速度（通常用 Hz 表示）。频率的倒数是周期（period）T，T=1/f。它是指信号重复一周所花的时间。相位（phase）是指一个周期内信号在不同时间点上的相对位置。

一般的正弦波可如下表示：

$$S(t)=A\sin(2\pi ft+\theta)$$

我们可以看一下振幅、频率和相位分别取不同值时的情况，如图 2.15 和图 2.16 所示。

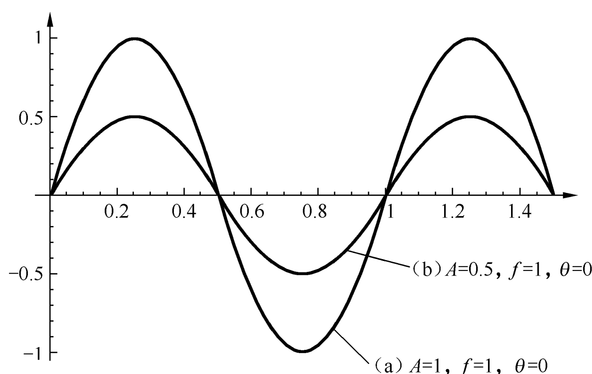


图 2.15　正弦波 $S(t)=A\sin(2\pi ft+\theta)$幅度变化

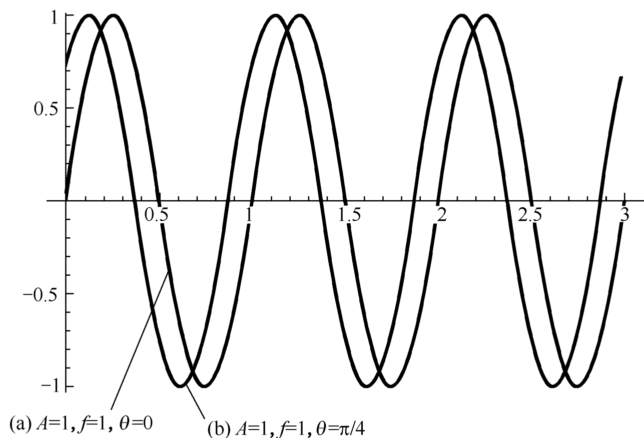


图 2.16　正弦波 $S(t)=A\sin(2\pi ft+\theta)$相位变化

2.3.3　信号的频域概念

频域的概念对于通信而言非常重要，属于非掌握不可的内容。

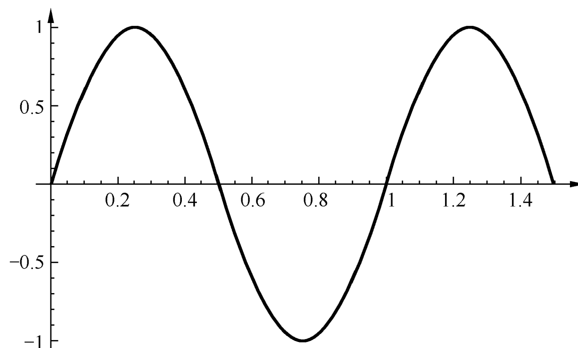
我们在 2.3.2 节中对正弦波做了一番简单的介绍，然而通常一个电磁信号会由多种



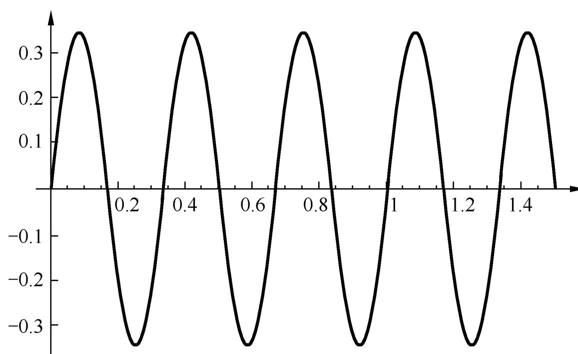
频率组成，而非单一的频率，比如说下面的信号：

$$S(t)=\sin(2\pi ft)+(1/2)\sin[2\pi(3f)t]$$

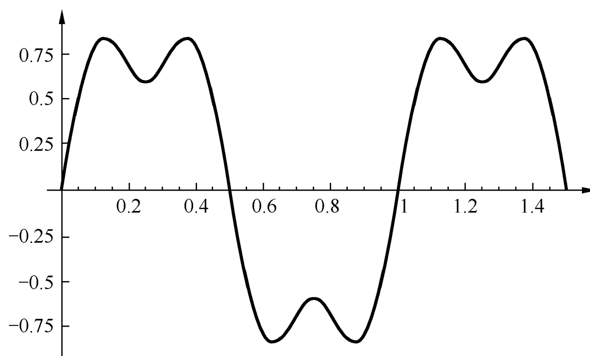
这个信号的组成成分只有频率为 f 和频率为 $3f$ 的正弦波，如图 2.17 所示。



（a）$\sin(2\pi ft)$



（b）$(1/2)\sin[2\pi(3f)t]$



（c）$S(t)=\sin(2\pi ft)+(1/2)\sin[2\pi(3f)t]$

图 2.17　频率成分的叠加（$T=1/f$）



这种频率成分的叠加会形成一个有意思的现象，如果我们给予每个谐波分量一个合适的系数，然后把这些谐波分量叠加起来，那么叠加的图形会越来越接近一个方波！

这个结论或许不是那么重要，但我们将它引申一下，提出一个思考题。作为周期信号的方波可以近似地用正弦信号及其谐波信号来表示，那么其他周期信号是否也具有同样的性质呢？

2.4 信号分析的利器——傅里叶级数和傅里叶分析

我们在上节对简单的正弦波做了介绍，但是这对实际工作的作用是非常有限的。因为无论是电磁信号还是声波信号，都不会是一个简单的正弦函数。上节所介绍的正弦函数的波形及一些性质，面对如图 2.18 所示的信号就会显得束手无策。

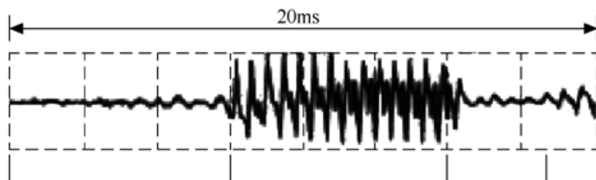


图 2.18　20ms 的语音信号

图 2.19 所示的是 20ms 的语音信号。在 GSM 通信系统中，通常以 20ms 为单位对信号进行抽取然后编码。分析这样的信号对目前的我们来说是困难的，因为我们还没有掌握分析信号的工具，就像手里没有斧子就砍不了大树一样。

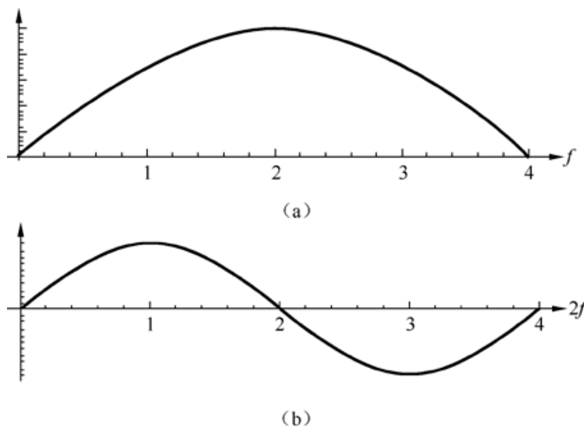


图 2.19　抖绳子的示例图



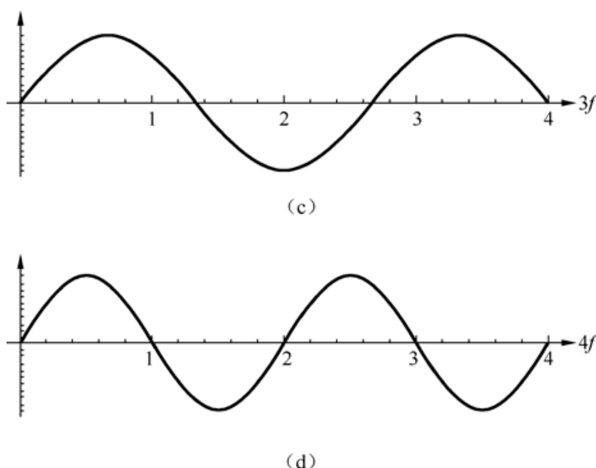


图 2.19　抖绳子的示例图（续）

这个毫无规律的信号看得我们头都大了，很不爽，总得先找个有点规律的开始研究，嗯，咱还是拿周期信号开刀，谁让你做一天和尚撞一天钟，简单呢。

对周期信号的分析研究，最早来自 1748 年欧拉对振动弦进行的研究工作。我们把绳子一头系在墙上，另一头拿在手里，然后用力抖绳子。那么在绳子上就会形成一个又一个的波，抖得越快的话，那么波浪就会越多，这样的生活体验相信大家都有过，如图 2.19 所示。

2.4.1　傅里叶级数与傅里叶分析的由来

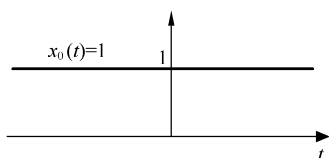
欧拉继续分析下去，发现所有的振荡模式都是 x 的正弦函数，并成谐波关系。欧拉得出的结论是：如果某一时刻振动弦的形状是其谐波的组合，那么在其后任何时刻，振动弦的形状也都是这些振荡谐波的组合。

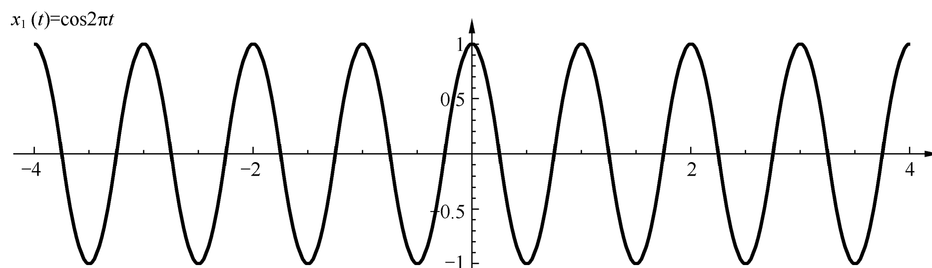
欧拉的结论很深奥，咱们用一句通俗的话说，那就是在绳子上滚动的信号，总可以表示为图 2.20 所示的一堆正弦波的叠加，至于每个正弦波所占的比重也就是系数咱另说。正弦函数和余弦函数也统称三角函数，在信号与系统中，往往习惯叫三角函数。

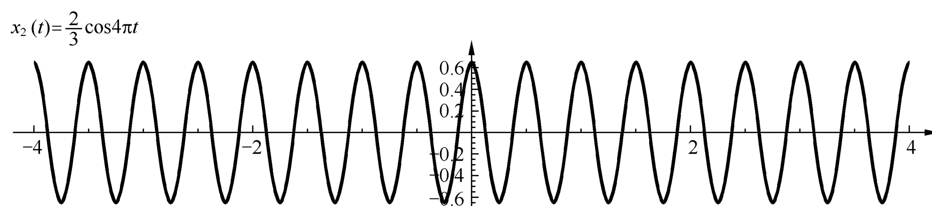
1753 年，伯努利声称一根弦的实际运动都可以用振荡谐波的线性组合来表示。

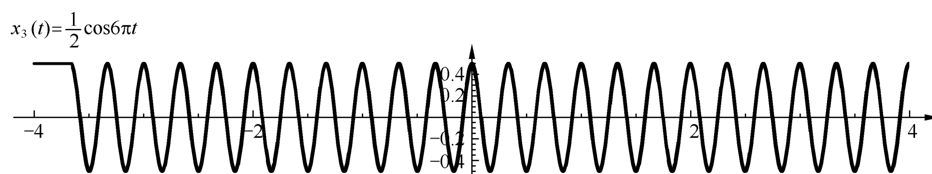
1759 年，拉格朗日提出了反对意见，他批评了使用三角级数来研究振动弦的主张，认为这个没多大用处。因为实际的信号往往有中断点的，不像绳子一样从头到尾都是完整的。那么有间断点的信号就像一根断了的绳子，你还能用三角级数来分析吗？











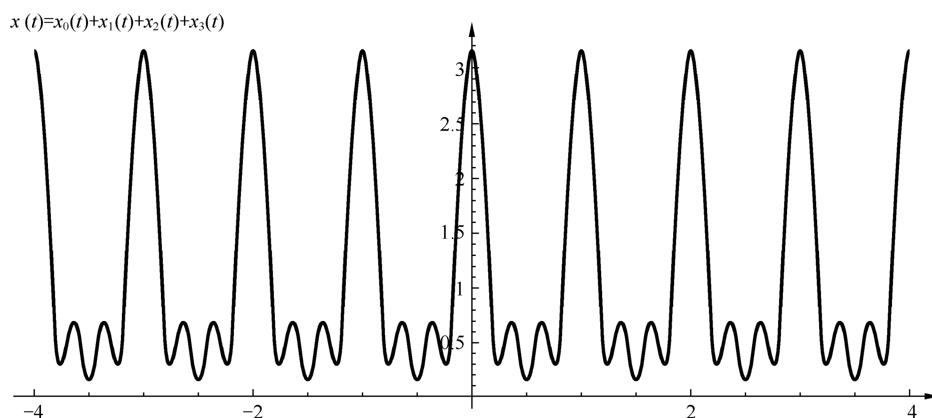


图 2.20　例 2.1 中 $x(t)$作为谐波关系的正弦信号的线性组合来构成的图解说明



这时候轮到我们的主人公傅里叶登场了。1807 年，傅里叶在进行热力学研究的时候发现，表示一个物体温度分布的时候，成谐波关系的正弦函数级数是非常有用的。这时候他提出了一个大胆的猜想：“任何”周期信号都可以用成谐波关系的正弦函数级数来表示？！

这个论述非常有意义，因为它适用范围非常广。傅里叶本人并没有给出详细的数学论证，这个命题后来是由狄里赫利给出完整的证明：在一定的条件下，周期信号可以用成谐波关系的正弦函数级数来表示。

另外，傅里叶还给出了非周期信号的表达方式：不是成谐波关系的正弦信号的加权和，而是不全成谐波关系的正弦信号的加权积分。

2.4.2　周期信号的数学表达——傅里叶级数

刚才我们说了在满足狄里赫利条件下，周期信号可以用成谐波关系的正弦函数来表示。我们知道，如果一个信号是周期的，那么对于一切 t，存在某个正值的 T，即

$$x(t)=x(t+T) \tag{2.1}$$

现在我们来考虑周期复指数信号（因为它在信号与系统中应用最广泛），即

$$x(t)=\mathrm{e}^{\mathrm{j}\omega_0 t}=\cos\omega_0 t+\mathrm{j}\sin\omega_0 t \tag{2.2}$$

我们很容易看出复指数信号是周期的，而且其基波频率为 ω_0，基波周期为 $T=2\pi/\omega_0$。那么与它成谐波关系的信号的频率就应该是它的 k 倍。可以得出式（2.2）中的复指数信号的一个成谐波关系的信号的集合，如下表示：

$$\phi_k(t)=\mathrm{e}^{\mathrm{j}k\omega_0 t}=\mathrm{e}^{\mathrm{j}k(2\pi/\mathrm{T})t} \qquad k=0,\ \pm1,\ \pm2,\cdots \tag{2.3}$$

这些信号都有一个基波频率，它是 ω_0 的倍数。因此每一个信号对周期 T 来说都是周期的。于是，由傅里叶的推论和狄里赫利的证明，可以得出一个由成谐波关系的复指数线性组合形成的信号，如下表示：

$$x(t)=\sum_{k=-\infty}^{+\infty}a_k\mathrm{e}^{\mathrm{j}k\omega_0 t}=\sum_{k=-\infty}^{+\infty}a_k\mathrm{e}^{\mathrm{j}k(2\pi/T)t} \tag{2.4}$$

在上式中，a_k 就是欧拉所说的加权系数，$\mathrm{e}^{\mathrm{j}k\omega_0 t}$ 就是欧拉所说的谐波信号。$K=0$ 这一项就是一个常数，$k=+1$ 和 $k=-1$ 这两项都有基波频率等于 ω_0，两者合在一起称为基波分量或一次谐波分量。$k=+2$ 和 $k=-2$ 这两项也是周期的，其周期是基波分量周期的 1/2，频率是基波频率的两倍，称为二次谐波分量。一般来说，$k=+N$ 和 $k=-N$ 的分量称为第 N 次谐波分量。一个周期信号表示成式（2.4）的形式，称为傅里叶级数。

我们在这里举一个例子来说明傅里叶级数到底有什么用途（如图 2.20 所示）。

例 2.1　假设有一个周期信号 $x(t)$，其基波频率为 2π，只要其满足狄里赫利条件，我们就可以把这个周期信号写成式 2.4 的形式，则为：

$$x(t)=\sum_{k=-3}^{+3}a_k\mathrm{e}^{\mathrm{j}k2\pi t} \tag{2.5}$$

其中 $a_0=1, a_1=a_{-1}=1/2, a_2=a_{-2}=1/3, a_3=a_{-3}=1/4$

我们将式（2.5）中具有同一基波频率的谐波分量合在一起以便于计算，得到下式：

$$x(t)=1+\frac{1}{2}(\mathrm{e}^{\mathrm{j}2\pi t}+\mathrm{e}^{-\mathrm{j}2\pi t})+\frac{1}{3}(\mathrm{e}^{\mathrm{j}4\pi t}+\mathrm{e}^{-\mathrm{j}4\pi t})+\frac{1}{4}(\mathrm{e}^{\mathrm{j}6\pi t}+\mathrm{e}^{-\mathrm{j}6\pi t})$$

我们对上式进行简化，可得

$$x(t)=1+\cos 2\pi t+\frac{2}{3}\cos 4\pi t+\frac{1}{2}\cos 6\pi t$$

$$x_0(t)=1$$

我们在本例中演示了一个周期信号是如何分解为基波信号和谐波信号之和的。试想一下，符合狄里赫利条件的周期信号都可以这样分解为一个个正弦信号的和，正弦信号又是我们非常熟悉的，那应付起来岂不是如庖丁解牛。话说正弦信号之和虽然有这么多项不是那么好处理，总比两眼一抹黑地去对付一个啥性质也不知道的周期信号要好吧。

所以说傅里叶级数其伟大的地方就在于，把一个看上去没什么规律的周期信号给规律化了（从数学上理解为基波信号和谐波信号的叠加），这样一来我们总算有了对付周期信号的数学工具。

且慢！！想必聪明的朋友已经发现了，我们在例 2.1 里回避了一个问题，那就是这些谐波在整个信号中所占的分量，也就是加权系数 a_k 到底是怎么得来的呢？

虽说我们现在已经知道了任意一个符合狄里赫利条件的周期信号都可以表述为 $x(t)=\sum_{k=-3}^{+3}a_k\mathrm{e}^{\mathrm{j}k2\pi t}$ 的形式，但是如果不告诉我 a_k 怎么得来的那还是白说，我还是没有办法将一个周期信号分解为不同的谐波分量啊。你不能光给世界观，不给方法论啊。

求这个系数的方法是有的，但是其数学证明却相当复杂，所以在这里我们略去证明过程，仅仅给出结论。希望对完整的证明过程有所了解的读者请参见参考文献 1 的第 3 章的有关内容。假设 $x(t)$为符合狄里赫利条件的周期信号，那么要将其分解为式（2.5）的形式，其系数的求法如下所示：

$$x(t)=\sum_{k=-\infty}^{+\infty}a_k\mathrm{e}^{\mathrm{j}k\omega_0 t}=\sum_{k=-\infty}^{+\infty}a_k\mathrm{e}^{\mathrm{j}k(2\pi/T)t} \tag{2.6}$$

$$a_k=\frac{1}{T}\int_T x(t)\mathrm{e}^{-\mathrm{j}k\omega_0 t}\mathrm{d}t=\frac{1}{T}\int_T x(t)\mathrm{e}^{-\mathrm{j}k(2\pi/T)t}\mathrm{d}t \tag{2.7}$$

式（2.6）称为综合公式，式（2.7）称为分析公式。系数 a_k 往往称为 $x(t)$的傅里叶级数系数或 $x(t)$的频谱系数。这些复数系数是对信号 $x(t)$中的每一个谐波分量的大小作出的



量度。系数 a_0 就是 $x(t)$的直流或常数分量。

> **提示：**我们在上面研究了周期信号的傅里叶表达方式，但是这对研究信号是不够的，因为很多信号是非周期的，比如本节开始图 2.18 所示的信号就不是周期的。本书中要研究的大多数信号，比如语音信号，也是非周期的。我们面对非周期信号是不是也有什么有效的方法来进行数学处理呢？或许有人要摩拳擦掌试图干出点什么，但是很不幸，这个问题也被傅里叶解决了，就是我们接下来要讨论的傅里叶分析。

2.4.3　非周期信号的数学阐述——傅里叶分析

傅里叶是这样看待非周期信号的，他认为一个非周期信号可以看作周期无限长的周期信号，正是这种颇具有哲学意味的观点填平了周期信号与非周期信号之间的鸿沟，从而拉开了傅里叶分析的序幕。

下面我们就试着用傅里叶级数的观点来对非周期信号进行探讨：首先回到式（2.6），当周期 T 增加时，基波频率 $2\pi/T$ 就减小，所以成谐波关系的各分量在频率上就越靠近。当周期变成无穷大时，这些频率分量之间就变得无限小，从而组成一个连续域，傅里叶级数的求和就变成了进行积分。

出于篇幅和内容的考虑，我们仅对傅里叶分析给出感性的认识，具体的数学证明过程，请参见本书参考文献 1 的第 3 章。

傅里叶分析的数学表达式为：

$$x(t)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}X(\mathrm{j}\omega)\mathrm{e}^{\mathrm{j}\omega t}\mathrm{d}\omega \tag{2.8}$$

$$X(\mathrm{j}\omega)=\int_{-\infty}^{+\infty}x(t)\mathrm{e}^{-\mathrm{j}\omega t}\mathrm{d}t \tag{2.9}$$

式（2.8）与式（2.9）称为傅里叶变换对，函数 $X(\mathrm{j}\omega)$ 称为 $x(t)$ 的傅里叶变换或傅里叶积分，式（2.8）称为傅里叶反变换。请分别比对式（2.6）与式（2.8）、式（2.7）与（2.9）的异同。

无论是傅里叶级数也好，傅里叶变换也罢，价值之一在于给我们提供了一个分析信号的工具，结合系统的一些特性，可以得出很多有用的结论。价值之二在于给了我们一个看待信号的全新的视角，我们以前都是从时域的角度来看待信号，把信号理解为时间上电平高高低低的连续变化，它是一个二维的坐标体系，两个维度分别是时间和电平值；现在我们可以从频域的角度上来理解信号，把信号理解为不同频谱的复指数信号的叠加，也就是基波分量和谐波分量的叠加，不同频率的谐波分量有着不同的权重系数，这也是一个二维的坐标体系，两个维度分别是频率和权重系数。

很多人对于时域到频域的转换难以理解，其实就是无法理解这两个坐标系的转变，我

们不妨举一个简单的例子做一下说明，体会一下“时域—频域”坐标系是怎么变化的。乔丹是篮球之神，他打篮球动作频率很快，这一秒可以做 4 个动作，下一秒可以做 3 个动作，下下秒可以做 5 个动作，下下下秒……我们首先看看这一句话如何用时域坐标系表示，如图 2.21 所示。

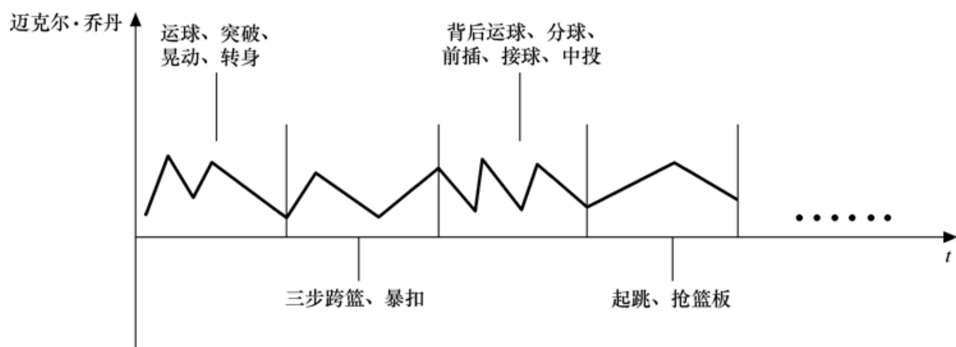


图 2.21　从时域的观点来欣赏迈克尔·乔丹

作为一个普通的观众，我们通常是从时域的观点来欣赏迈克尔·乔丹，看看他这秒干了什么，下一秒又做了哪些精彩的动作。

可是偏偏还有这么一群人，他们目光深邃，表情冷峻，他们对篮球场上那些华丽的诗章毫无兴趣，他们根本就不用时域的观点来欣赏迈克尔，他们用频域!!! 这些人是干嘛的呢，他们是球队的技术分析，他们统计迈克尔每秒都做了多少动作，用频域的观点来分析迈克尔能给球队带来多少胜利。这群人毫无疑问是欧拉和傅里叶的崇拜者，估计对伯努利和拉普拉斯也是仰慕有加，要不你没法解释他们为什么要这么做，我们来看看这群人是怎么来分析迈克尔·乔丹的（如图 2.22 所示）。

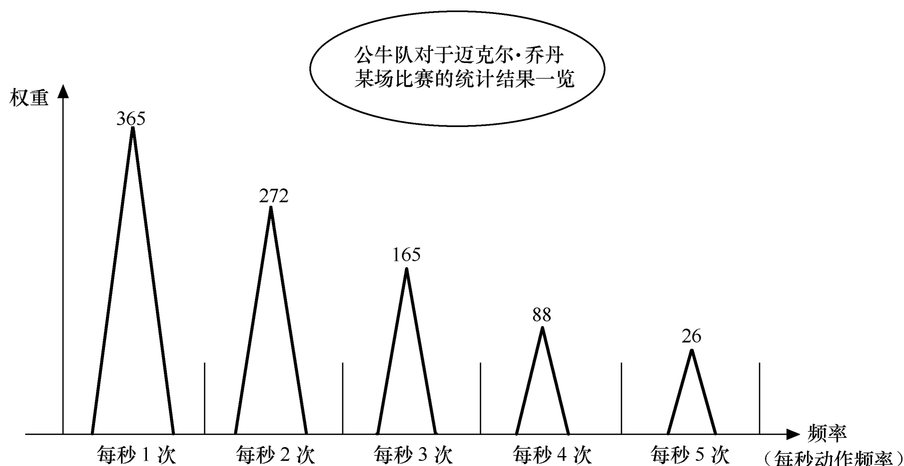


图 2.22　从频域的观点来欣赏迈克尔·乔丹



傅里叶级数实现从时域到频域的变换也类似于此，迈克尔一场比赛打的时间的长短只是影响各个动作频率在图 2.22 中的权重而已。信号在时域上的不断延伸只不过是改变各个谐波分量的权重值而已，频域上不需要时间这个维度，时间上的变化在这里转换成了权重上的变化。

2.5 模拟信号如何转变为数字信号

本书重点要关注的是以蜂窝通信为基石的无线通信，无论是 GSM 也好、CDMA 也罢，这些现代无线通信系统有一个共同的特点，那就是它们采用的都是数字制式。在现阶段，数字通信系统相对模拟通信系统有着巨大的优势，这个问题已经在 2.2 节中讨论过了。可是问题也就随之而来了，我们说话的语音信号是声波，属于模拟信号，我们打视频电话，影像是光波，也属于模拟信号，而中间采用的通信系统却是数字通信系统，那么就必定有一个从“模拟信号”到“数字信号”的转变过程。

这个从模拟到数字的转换包含了“采样”、“量化”两大过程，这两大过程是为了让模拟信号流转变成比特信号流。通常情况下，为了更有效率地表达我们想表达的内容，我们还需要对其进行“编码”。

2.5.1　声音是如何变成比特流的——奈奎斯特采样定理

2.4 节中图 2.18 所示为一个 20ms 的语音信号，这样一个信号是如何转变为“0”、“1”交错的比特流的呢，这就是本小节要讨论的内容。

大家回忆一下我们在初中时画正弦曲线 y=sin$x$ 的时候是怎么做的，老师会要求我们尽量多地描出一些点，比如（0，0）、（π/6，1/2）、（π/4，$\sqrt{2}$/2）等，在坐标轴上描图，然后用光滑的曲线把这些点连接起来，就成了连续的正弦函数曲线图。

我们使用的“模拟—数字”变换技术与上述过程有异曲同工之处，从时间轴上等间隔地取 N 个时间点，然后取 N 个值，这个过程称为“采样”。

问题就来了，究竟要取多少个点，原有的连续时间信号所含的信息才不会丢失，才能完整地保留下来，然后被还原？

凭我们的第一直觉，往往认为肯定需要无穷个点才能保证信号能不被丢失地还原，也就是采样频率为无穷大。然而，奈奎斯特却给出了一个论证，他证明了如果一个信号是带限的（即它的傅里叶变换在某一有限频带范围以外均为零），如果采样的样本足够密的话（采样频率大于信号带宽的两倍），那么就可以无失真地还原信号。这个结论被称为奈奎斯特采样定理。



对于奈奎斯特采样定理，有着严格的数学证明，请参见参考文献 1 的第 7 章。在这里仅举一个实际的例子，让大家对此有一个直观的认识。

看电影的时候，电影播放的画面是连续的吗？和眼睛直接看该场景会是一样的吗？非也，电影里的世界和我们眼睛里直接看到的世界是有差别的，匪夷所思吧。

电影播放的实际不是连续画面，而是由一张张的胶片或者说一帧帧的画面组成的，其中每一帧都代表着连续变化景象中的一个瞬时画面（也就是时间样本）。当以足够快的速度来看这样连续的样本时，我们就会感觉到是原来连续活动景象的重现，一般情况下每秒要采集多少样本，眼睛才会觉得这是连续的画面呢？电影的通常做法是每秒播放 24 帧，也就是说采样频率是 24 就够了，眼睛会对画面有一个非常短暂的“视觉停留”，这相当于对样本信号的一个内插来还原原信号的过程。所谓“内插”，用中学数学的话来说就是把你刚才描的点用线连起来，形成了一个函数的图形。下面用图 2.23 来表述眼睛对电影画面的“内插”的原理。

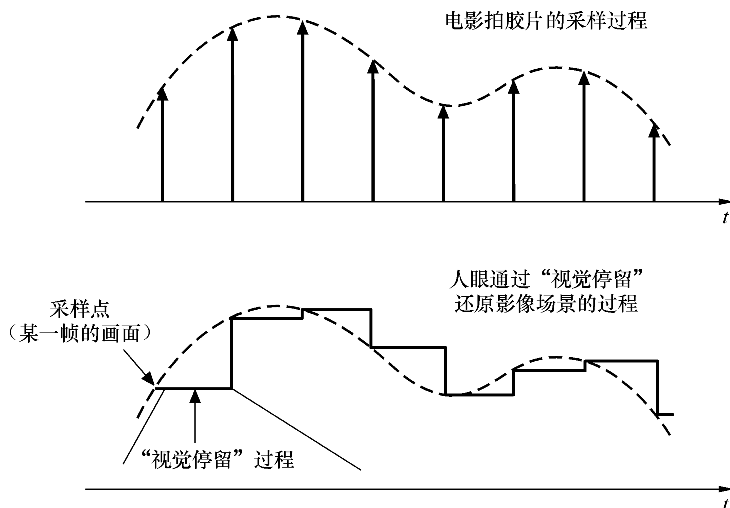


图 2.23　电影的 24 帧与人眼的“视觉停留”

图 2.26 中的“内插”或者说“视觉停留”用“信号与系统”的话说就是“零阶保持”了。

话说这 24 帧的采样频率真的是够吗，对于绝大多数情况下是够了，不过有一种情况下可能就不够了。比如说马车的轮子，要是这个轮子运动得飞快，一秒不止转 12 圈的话，也就是说 24 帧采样频率不够的话，那么问题就来了，在电影中甚至会看到轮子朝运动的相反方向转动的情况，相信很多人有过这样的体验。我们称这种情况为“欠采样”，那么这个情况是怎样发生的呢？请看图 2.24。



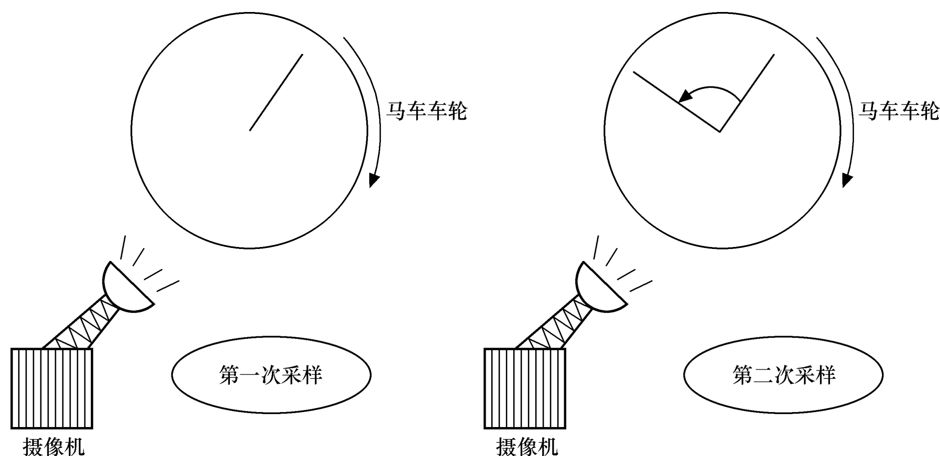


图 2.24　电影拍摄时候马车车轮的转动情况

摄像机每秒拍摄 24 帧画面，也就是 24 张胶片。我们假设马车轮每秒转动 18 圈，那么采样频率就达不到 2 倍频，就会出现“欠采样”的情况，不能完整地反映马车的运动情况。

两次采样的间隔是 1/24s，马车轮是顺时针转动的，在此段时间内可以转动（1/24）×18=3/4 圈，也就是说顺时针转动 270°，然而从人眼中看就好像是逆时针转动了 90°一样，从而造成了轮子反着转的错觉。术语也称之为“混叠”。

那么奈奎斯特采样定理对我们将语音的模拟信号转换为比特流有什么实际的意义呢？

人发出的声音的频率一般为 85～1 100Hz，而 1～4kHz 也是人耳非常敏感的频率范围。奈奎斯特采样频率选定为 8kHz 就基本可满足手机通话的需求，实际上，GSM 规范规定的 GSM 手机采样频率正是 8kHz。

2.5.2　从原始分到标准分——量化

奈奎斯特采样定理其意义在于它提供了从连续时间信号向离散时间信号转换的通道，使得利用离散时间系统技术来实现连续时间信号成为可能。但奈奎斯特采样得出来的结果，只能称为“离散时间信号”而不是真正意义上的“数字信号”。

道理很简单，像图 2.23 的采样，其采样值还是随信号幅度连续变化的，即采样值 m（kT）可以取无穷多个可能值。假设要用一个 N 位二进制位组来表示该数值的大小，以便对该信号进行数字化处理，但是 N 位二进制比特只能表征 $M=2^N$ 个电平值，而不能与无穷多个电平值相对应。这样一来，采样值必须被划分为 M 个离散电平，此电平被称作

量化电平。

可以这样说，采样的作用是把一个时间连续信号变成时间离散的信号，而量化则是将取值连续的采样变成取值离散的采样。

量化也分为两种，一种是均匀量化，另一种是非均匀量化。

1. 均匀量化

把输入信号的取值等距离分割的量化称为均匀量化，如图 2.25 所示。这种量化方式有点像当年的标准分制，我国以前采取过 5 分制，把 81～100 的原始分规定为 5 分，61～80 规定为 4 分，41～60 规定为 3 分，21～40 规定为 2 分，1～20 规定为 0 分，颇有点优秀、良好、及格、不及格这种粗略评价的感觉。

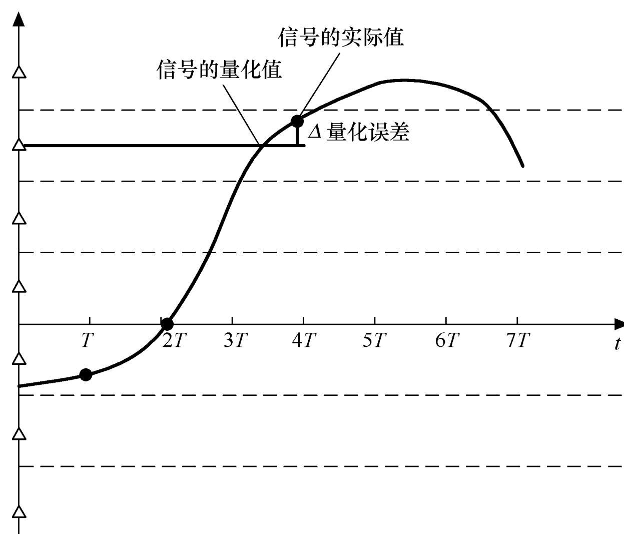


图 2.25　均匀量化示意图

我们在图 2.25 中将纵坐标划成均匀的一个个的区间，每个区间的间隔称为量化间隔 Δv，每个区间的中值取为量化电平。量化间隔取决于输入信号的变化范围和量化电平数。以上两个参数确定后，量化间隔也被确定。例如，假如输入信号的最小值和最大值分别用 a 和 b 表示，量化电平数为 M，则：

$$\Delta v = \frac{b-a}{M}$$

量化的好处是方便进行数字处理，代价是产生了失真，也就是图 2.25 所示的量化误差。这种失真也通常称为量化噪声。量化噪声由量化前的连续随机变量与量化后的离散



随机变量的均方差来进行度量。

2. 非均匀量化

均匀量化有一个比较要命的问题，那就是对于小信号而言误差比较大，信噪比的结果比较差劲，这个事情怎么说呢，下面举一个例子进行说明。

假设一个信号的变化范围为[0，10]，量化电平数为 10，那么取每个区间的中值为量化电平，就分别为 0.5，1.5，2.5，…，9.5。

那么对于小信号 0.9，在第 1 个区间里，所以其量化电平为 0.5，那么其信号功率为 $S_0=(0.9)^2=0.81$，量化噪声功率为 $N_0=(0.9-0.5)^2=0.16$，因此信号与量化噪声功率比为：

$$\left(\frac{S_0}{N_0}\right)_{\text{dB}}=10\lg\left(\frac{0.81}{0.16}\right)\approx 7\text{dB}$$

那么对于大信号 9.9，在第 10 个区间里，所以其量化电平为 9.5，那么其信号功率为 $S_0=(9.9)^2=98.01$，量化噪声功率为 $N_0=(9.9-9.5)^2=0.16$，因此信号与量化噪声功率比为：

$$\left(\frac{S_0}{N_0}\right)_{\text{dB}}=10\lg\left(\frac{98.01}{0.16}\right)\approx 27\text{dB}$$

由此可以看出，均匀量化对于小信号而言，其信噪比太低，远远低于大信号的信噪比，而对于语音信号而言，一般又是小信号居多。这种现实的矛盾使得均匀量化越来越不适合于通信应用，于是就导致了非均匀量化的诞生。

实际中非均匀量化的实现方法通常就是将采样值经过压缩后再进行均匀量化。所谓压缩就是用一个非线性变换电路将输入变量 x 变换成另一个变量 y，即 $y=f(x)$。非均匀量化就是对压缩后的变量 y 进行均匀量化的过程。

通常使用的压缩器中，大多采用对数式压缩，即 $y=\ln x$，目前美国采用的是μ律压缩，我国和欧洲采用的是 A 律压缩，下面就来介绍一下 A 律压缩。

所谓 A 律压缩就是压缩器具有如下特性的压缩律：

$$y=\frac{Ax}{1+\ln A},0<x\leqslant\frac{1}{A}$$

式中，x 为归为一化的压缩器输入电压；y 为归一化的压缩器输出电压；A 为压扩参数，表示压缩程度，在实际中，往往选择 A=87.6。

由于在电路上实现这样的函数规律极其复杂，所以在实际应用中通常采用近似于 A

律函数规律的 13 折线（A=87.6）的压扩特性，13 折线的示意图如图 2.26 所示。

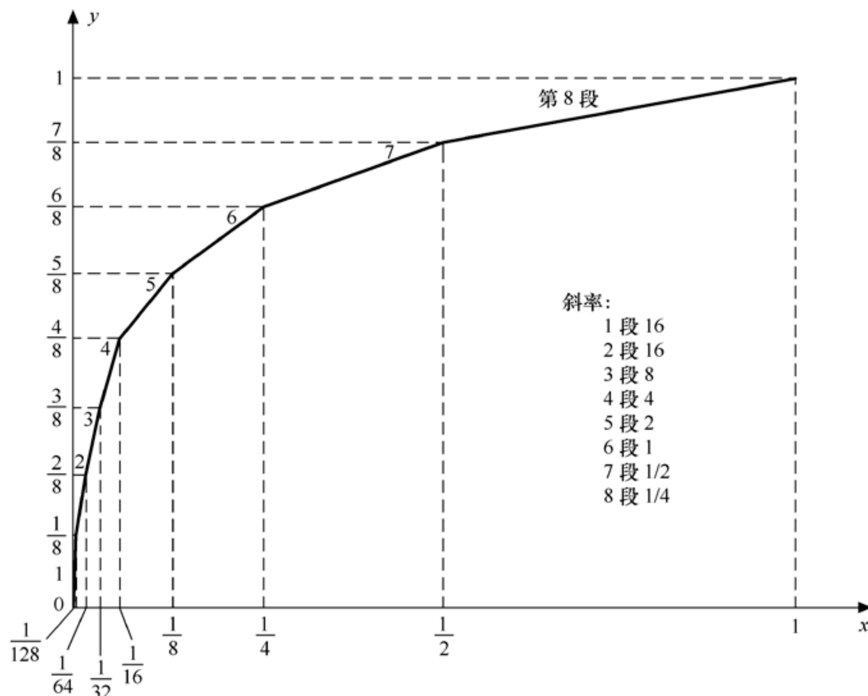


图 2.26　13 折线示意图

由图中可以看出，y 轴实际上是 x 轴的函数，是 x 轴的非均匀映射，通过这种方式，就可以通过 y 轴的均匀量化实现 x 轴的均匀量化。

上面所述的是发射端的压缩，至于接收端对信号的扩张，实际上就是压缩的反过程。

2.5.3　从《蒹葭》和《在水一方》说起——也谈编码

经过了奈奎斯特采样和非均匀量化后，就得到了我们想要的比特流了吗？No！经过量化后我们只不过得到了一堆量化电平值，怎么对这些量化电平进行编码让其变成比特流，那还是一件颇伤脑筋的事情。

无论采取哪一种编码，它描述的都是一个连续时间的语音信号在离散域上的映射，反正描述的东西都是一个，我们自然希望编码越简单越好，效率越高越好。

说到编码，在本小节中的意思就是将量化电平转化为二进制比特流的过程。其实作者认为完全不必理解得这么狭义，可以从更广的视角来理解编码。比如说语言就是对人



类的事物和情感进行的编码，对于同一件事情，在人类世界可能有多种编码（语言）与之对应。比如说我爱你，英语的编码就是“I love you”，法语的编码是“je t'aime，je t'adore”，德语的编码是“Ich liebe dich”，意大利语的编码是“Tiamo”。与此类似的，对于同一个量化电平，也可能有多种编码方式，比如说 PCM、ΔM、DPCM，它们用各自不同的方式来阐述同一个量化电平。

编码有一个很重要的问题就是效率问题，通信系统的资源是宝贵的，自然希望对一个量化电平的阐述能够尽量节约一点，占用少一点的电平。下面用一个稍微夸张一点的例子说明什么是编码的效率。

当你在河边漫步的时候，无意间发现一位佳人，一袭白裙飘飘，清新脱俗，温婉可人，令你心生爱慕，相思难断，你打算如何用文字（编码）来表达你的这份思绪呢？

琼瑶和《诗经》分别用《在水一方》和《蒹葭》给出了不同的答案。



《在水一方》
绿草苍苍/白雾茫茫/有位佳人/在水一方
我愿逆流而上/依偎在她身旁/无奈前有险滩/道路又远又长
我愿顺流而下/找寻她的方向/却见依稀仿佛/她在水的中央
《蒹葭》
蒹葭苍苍/白露为霜/所谓伊人/在水一方
溯洄从之/道阻且长/溯游从之/宛在水中央

单从编码效率而言，《在水一方》和《蒹葭》高下立判，至于诗词的优美程度，那就不是本节需要评判的内容了。

下面我们来讨论一下 PCM 编码和 DPCM 编码，看看后者相比前者作了哪些改进从而提高了编码效率。

1. PCM 码

值得注意的是，真正的通信系统中应用的 PCM 编码是采用 A 律 13 折线法的，用 8 个 bit 位来表征，共可以表示 2^8=256 个电平。为了简便起见，我们用 4 个 bit 位的 PCM 编码来说明问题。4 个比特可以表征 16 个量化电平，最高位比特设置为极性码，当电平值为正时取“1”，为负时取“0”，如图 2.27 所示。

图 2.27 中共有 16 个量化区间，其量化间隔为 0.5V，各个量化区间的判决电平依次为−4V，−3.5V，…，3.5V，4V。16 个量化电平分别为−3.75V，−3.25V，…，3.25V 和 3.75V。图 2.27 显示了 12 个采样值电平，下面对它们进行编码（如表 2.1 所示）。

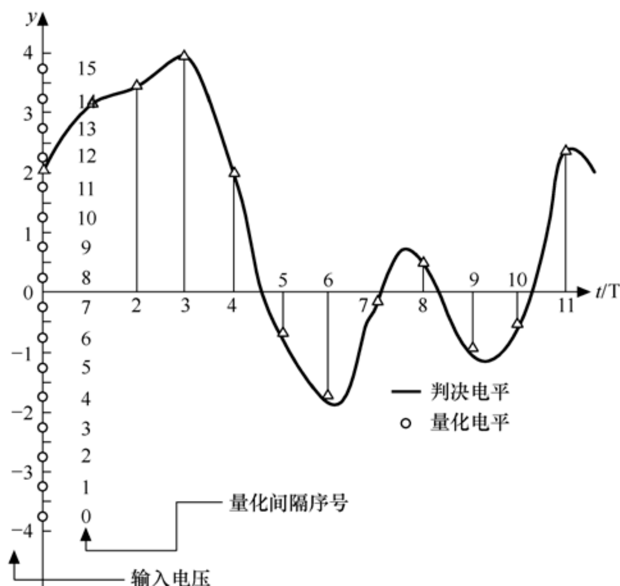


图 2.27　PCM 量化与编码

表 2.1　　　　　　　　　　　　　　PCM 量化与编码

采样时间	6T	5T	7T	8T	4T	0T	1T	2T	3T
采样值	−1.76	−0.75	−0.2	0.4	1.9	2.1	3.2	3.4	3.9
量化电平	−1.75	−0.75	−0.25	0.25	1.75	2.25	3.25	3.25	3.75
二进制编码	0100	0110	0111	1000	1011	1100	1110	1110	1111

请注意，凡负电平其高位都是 0，凡正电平其高位都是 1，所以最高位也称作极性码。

2. DPCM（差分编码调制）

我们发现，在 PCM 体系中，每一个采样都是独立量化的，前面的采样值跟后面的量化没有什么关系。实际上，对于语音信号这种非突变信号，这样做是比较浪费的。当语音信号这样的带限信号以奈奎斯特速率或者更高的速率进行采样时，采样值通常是相关的随机变量。也就是说，如果前一个采样值很小，那么下一个采样值很小的概率就很大。如果用差值而不是绝对值进行编码，那么会更有效率。

比如说增量调制 DM 就是 DPCM 方案中的一个版本。在增量调制中，量化器采用的



是幅度为±Δ的 1 比特量化器。

如何在发射端形成 $f(t)$信号并编制成相应的二元码序列呢？仔细分析一下图 2.28，比较在每个采样时刻Δt 处的 $f(t)$和 $f(t-1)$的值，可以发现：

当 $f(t)>f(t-1)$时，上升一个σ，发“1”码；

当 $f(t)<f(t-1)$时，下降一个σ，发“0”码。

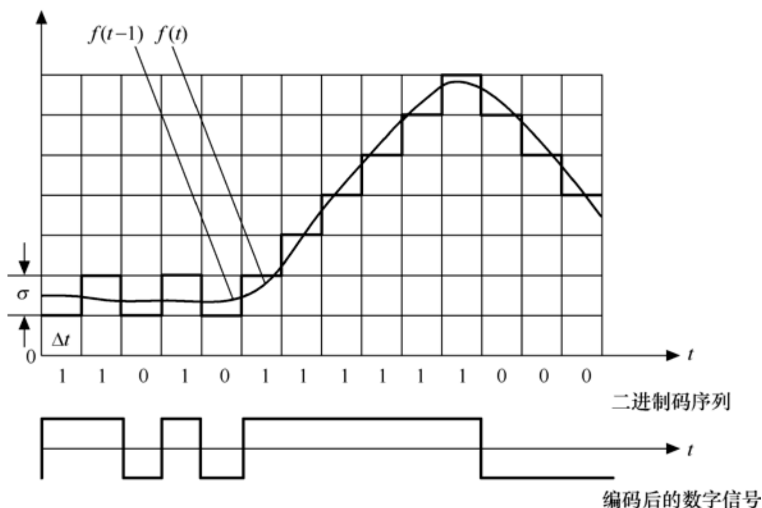


图 2.28　增量调制示意图

刚刚所说的 PCM 和 DPCM 编码都属于信源编码中最简单的编码，那什么叫信源编码？信源编码又有什么作用？

信源编码是以提高通信有效性为目的的编码。信源编码的效率通常是通过压缩信源的冗余度来实现的，比如说《在水一方》相对《蒹葭》就有冗余度，那么用信源编码的挑剔的眼光来看，表达同样的信息量前者占用了更多的比特位，那么它就不是一个好的信源编码。

概括一点地说，信源编码追求的是相同信息量的最少比特位。

可是在一个通信系统中要能完成端对端的信号传递，光有信源编码是不够的。这句话有点令人匪夷所思，因为我们刚刚说了只要进行奈奎斯特采样就可以把原始信号无遗漏地完全表述清楚了，为什么这样做还不够？下面简单类比一下。

对于一个通信系统而言，我们可以把它类比成一个教育体系，先且假设发送端是老师，接收端是学生。我们知道，教学体系追求的目标就是让学生完全听懂老师所讲的，那么通信系统追求的就是让接收端无差错地收到发送端发出的信号。

老师的讲课内容可以比作信源编码，一个是对知识的表述方式，一个是对信号的

表述方式，没有本质的区别。这样一类比你就会发现，很遗憾，光靠老师的讲课内容是无法达成教育体系的目的的，你上课可能走神，可能有东西没听懂，还可能有东西你没听懂但自以为听懂了，你怎么能保证光凭听课就能保证教学体系的终极目标——完全弄明白老师所讲的内容呢？所以，老师除了授课以外，还安排课后习题让学生自我验证到底学懂了没有。对于通信系统而言也是如此。信源编码在传输过程中可能丢失，可能发生信号变化，比如某些比特从“0”变为“1”，某些比特从“1”变为“0”，你光靠信源编码怎么能达成让接收端无差错地收到发送端发出的信号的终极目的呢。为了达成这个目的，我们就在信源编码的基础上，另外安排了一些冗余的比特当作课后习题一样传给收端，让收端自行验证信息是不是都收对了，这些“冗余信息”就称为信道编码。

信道编码是以提高信息传输的可靠性为目的的编码。通常通过增加信源的冗余度来实现。这与信源编码的追求恰好相悖，看起来像是信源编码辛辛苦苦省吃俭用现在轮到信道编码来败家。其实信源编码和信道编码其本质追求都是相同的，都是为了实现信号最有效的传输，只不过一个关注的是冗余度，一个关注的是有效性而已。话说现在又有了联合编码，即信源编码和信道编码不再分开而是进行统一编码，这算是一种新的尝试，但是这种方式尚不流行。

下面来关注信道编码的实现，即要怎么设计我们的课后题才能达到让接收端无差错收到发端信号的目的。

通常这些课后题的设计分为以下 3 种。

（1）检错重发法：接收端在收到的信码中检测出错误时，立即设法通知发送端重发，直到正确接收为止。也就是说你通过做课后习题发现老师讲的有些内容你理解得不对，于是要求老师再讲一遍，直到你明白为止。

（2）前向纠错法：接收端不仅能在收到的信码中发现有错码，还能够纠正错码。对于一个二进制系统，如果能够确定错码的位置，就能够纠正它，这很好理解，因为二进制就“0”和“1”两个数字，非此即彼。这种方法不需要反向信道（传递重发指令），也不会反复重发而延误时间，实时性好。这种方法就好比你通过做课后习题发现有些知识是你听错了，自己琢磨着就校正过来了。

（3）反馈校正法：接收端将收到的信码原封不动地转发回发送端，并与原发送信码相比较。如果发现错误，则发送端再进行重发。这种方式效率相当低，一般不怎么用，相当于你把老师讲的课再讲一遍给老师听，她认为没错那么你就没有错。

信道编码在通信中是一个非常重要的课题，与此相关的研究也层出不穷，比如线性分组码、卷积码、Turbo 码、奇偶校验码等。在这里，作者并不打算展开论述这些内容，而只打算讲讲原理，这么一大串“001010101111100100１”的比特流，它是如何发现自身



的错误的，又是如何完成检错的？初看起来有点令人不可思议，继而脑子里一片混沌，有点难以理解，我们还是举个例子来说明吧。

假如有一个 3bit 的编码，那么是可以表示 2^3=8 种编码的。现在我们只用它的两位来表征信息，另一个 bit 作为校验码，那么我们可以表示 2^2=4 个信息。如下所示：

$$\begin{cases} 000=\text{风} \\ 011=\text{雨} \\ 101=\text{雷} \\ 110=\text{电} \end{cases}$$

我们在这里拿最高位作为监督位，后两位作为信息位，也就是“000”表示风，“011”表示雨，“101”表示雷，“110”表示电。其实表征信息两个比特就完全够了，另一个比特是用来进行检错的。

上面任意两个码元都有两位是不同的，那么如果上述某一个信息元一个比特出了问题，都可以检测出来。比如“000”风，如果某一位比特出错，比如变成了“001”或者“010”，那么很快就可以发现在编码体系里没有这个编码，就说明这个码出错了，这就是检错。哪怕只是错了 1 个比特位，上述这种编码方式也是无法自行进行纠错的，比如“100”就是一个错误的信息，但你说它是由“110”错了 1 个比特，还是“101”错了一个比特呢，只知道错了，但是无法进行纠正。

为了纠错，我们不得不再增加冗余比特，如下所示：

$$\begin{cases} 000=\text{风} \\ 111=\text{电} \end{cases}$$

本来表征两个信息只要一个比特就够了，在这里，我们增加了两个比特作为监督位，这样一来，可以实现对 1 个比特错误的纠错。比如出现了“100”的码型，不用说，肯定是 000 的高位发生了错误，因为“111”的码型只错一位是无论如何不会变成“100”的。

在这里我们简单地介绍了一下检错和纠错的原理，如果要进行深入地学习，请参见通信原理的相关教材。

2.6　这是多此一举吗——也谈调制的意义

话说采样、量化、信源编码、信道编码都讨论完了，按照 2.2 节勾勒出来的框架，就该轮到调制了。所谓调制，就是频谱的搬移，以 GSM 为例，你们说话不是工作频率在 200～3 400Hz 吗，那好，我把你们搬迁到 900MHz 上去，这个频谱搬移的过程就称为调制。

这看起来很像吃饱了饭没事做，我在 4kHz 以下频段不是混得好好的吗，你干嘛非要把我搬到那么高的频段上去呢？把基带信号（4kHz 以下的语音信号）转变为频带信号（900MHz）真的有这个必要吗？这样做到底有什么好处呢？

（1）调制技术首先是为了和信道匹配。比如说无线通信中，走的信道就是大气层。对于大气层而言，音频范围（10Hz～20kHz）的信号传输将急剧衰减，而较高频率范围的信号可以传播到很远的距离。所以说要想在依靠大气层进行传播的通信信道上传输像语音和音乐这样的音频信号，就必须在发射机里将这些音频信号嵌入到另一个较高频率的信号里去。

（2）电磁波的频率与天线尺寸要匹配，一般天线尺寸为电磁信号的 1/4 波长为佳。调制可以用来将频带变换为更高的频率，从而减小天线的尺寸。初看这一点没觉得有什么，算算就知道有多吓人，以 4kHz 的语音信号为例，那么合适的天线尺寸是多少呢？

[(3×10^8m/s)/4 000 次/s]×1/4=18 750(m)，这么高的天线，会把飞机撞下来的!!

（3）在高频段更易于采用频分复用，我们一路语音信号就要占用 64kHz，低频段是没有这么多资源可以如此奢侈的。

下面来讨论一下如何进行调制，由于目前的蜂窝通信均是采取的数字通信技术，因此以下仅仅介绍一下数字调制。

话说我们经过“采样—量化—信源编码—信道编码”得到了一长串的“0101101011”的比特流，该怎么把这串比特流的信息嵌入一个电磁波中，从而在空中发送出去呢？这个信息嵌入的过程称为调制。试想一下，一个电磁信号可以用一个正弦波来表达，而正弦波无非就是 3 个参数：振幅、频率和相位。想把你的比特流信息镶嵌进去，也只能从这 3 个参数上打主意，别无它法。所以将数字数据转换为电磁信号的基本编码或者说调制技术相应也有 3 种，分别是：幅移键控（ASK，Amplitude Shift Keying）、频移键控（FSK，Frequency Shift Keying）和相移键控（PSK，Phase Shift Keying）。

图 2.29 非常重要，但是或许一下看不明白是怎么回事，我们来逐一看看这 3 种调制方式的表达式就知道了。

1. 幅移键控（ASK）

刚刚说了一个载波的三要素：振幅、频率、相位。这算是从第一要素振幅上在打主意，如何用振幅来表示“0”和“1”两个比特位呢。通常 ASK 方式是采用一个振幅值为 0 的载波来表示比特“0”，用一个振幅值恒定的载波来表示比特 1，如图 2.29（a）所示。结果得到信号的表达式为：

$$\text{ASK}\quad s(t)=\begin{cases}A\cos(2\pi f_{\text{c}}t) & \text{二进制数1}\\ 0 & \text{二进制数0}\end{cases}$$



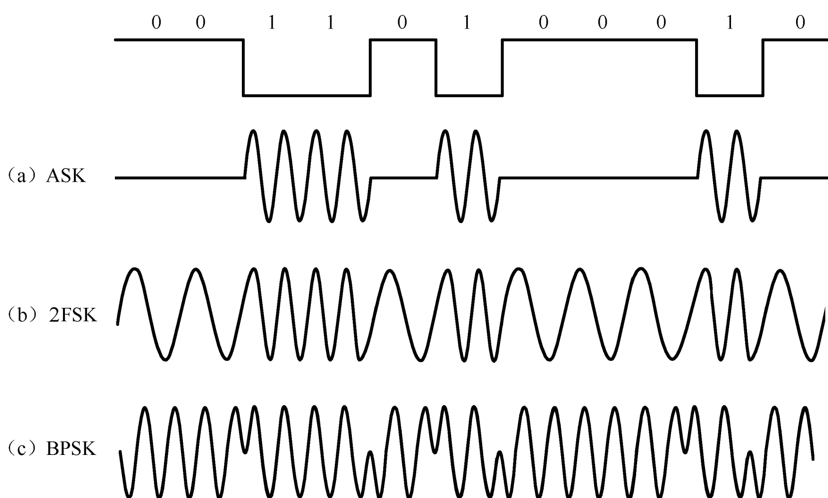


图 2.29　数字调制示意图

式中，载波信号为 $A\cos(2\pi f_c t)$ 。

幅移键控有一个缺点就是容易受到突发脉冲的影响。

2. 频移键控（FSK）

GSM 采用的调制方式 MSK 就是 FSK 中的一种。

频移键控最常见的形式是二进制频移键控（2FSK），它是用载波频率附近的两个不同的频率来表示两个二进制值，请参见图 2.29（b）。表示“0”和“1”的信号的两个载波的频率明显不同，表示“1”的载波的频率要高。信号的表达式如下：

$$\text{2FSK}\quad s(t)=\begin{cases}A\cos(2\pi f_1 t) & \text{二进制数1}\\ A\cos(2\pi f_2 t) & \text{二进制数0}\end{cases}$$

2FSK 的抗干扰能力要比 ASK 强。

3. 相移键控（PSK）

相移键控是无线通信中采用得比较多的，其数据通过载波信号的相位偏移来表示。

最简单的方式是两相相移键控（BPSK），它使用两个相差 180° 的相位来表示两个二进制数，请参见图 2.29（c），“0”信号和“1”信号的表达式如下：

$$\text{BPSK}\quad s(t)=\begin{cases}A\cos(2\pi f_c t+0) & = A\cos(2\pi f_c t)\\ A\cos(2\pi f_c t+\pi) & =-A\cos(2\pi f_c t)\end{cases}$$

由于 180° 的相移等于将正弦波的值乘以−1，那么就得到了上式。

2.7 信道与信道容量

曾几何时，电视上有这么一个广告："信道好才是真的好"。一时间人们互相都问："你手机的信道好不好？移动、联通的信道好不好？"

对于一个学通信的人而言，看到这种情景有点哭笑不得的感觉。因为人们口中的"信道"实际上指的是接收电平（信号的格数），真正的信道是指信号传送的通道，或者说信号的传输媒质。手机的信道都是空气，这部手机和另外一部手机的空气难道还不一样了，何来信道好不好之说？

信道又可分为有线信道和无线信道两类。有线信道包括明线、对称电缆、同轴电缆及光缆等。而无线信道有地波传播、短波电离层反射、超短波或微波视距中继。有时候，信道的定义不单单指传输媒质，还包括相关的变换装置（如发送设备、接收设备、调制器、解调器），我们称这种扩大范围了的信道为广义信道。

信道是多种多样的，信道上是有噪声的，我们通常关注的是，这些噪声会对传输信号的速率会产生多大的限制。我们把信道上可以被传输的最大速率称为信道容量（Channel Capacity）。对于信道容量而言，通常有以下几个概念。

（1）数据率（data rate）：数据能够进行通信的速率，用 bit/s 来表示。

（2）带宽（bandwidth）：指的是传输信号所占的带宽，用 Hz 来表示。我们在日常生活中又常常把数据率（bit/s）称作"带宽"。所以很多人头脑里经常有两股截然不同的势力在打架：一股是来自书本，它告诉你"Hz"才是带宽；另一股来自生活，它告诉你"bit/s"就是带宽，我们需要举一个例子来分清楚这两个概念。

以 GSM 为例，它的某一个频道的中心频率是 890.2MHz，那么它的频率范围就是[890.1MHz，890.3MHz]，共 200kHz，这 200kHz 就是真正意义上的"带宽"，指的是频带宽度，即频谱宽度！在这个频带上，如果传送的是 TCH 语音信号的话，那么调制速率就是 33.8kbit/s，这就是 GSM 传输的数据率（data rate）。数据率通常是小于信道容量的，一个信道的容量在没有噪声的理想状态下可以由奈奎斯特定理测算出来，在有噪声的情况可以由香农公式测算出来。这 200kHz 的带宽能承载的最高数据率是多少，可以根据信噪比计算出来。

（3）噪声（noise）：我们所讨论和关心的是通信线路上的平均噪声电平，关注的是统计学上的意义，而非单个的突发噪声。

（4）误码率（error rate）：即差错发生率，比如发送的是"0"而接收的是"1"，或者发送的是"1"而接收的却是"0"。



2.7.1　无噪声的完美信道——奈奎斯特带宽

首先值得注意的是，奈奎斯特带宽指的是信道无噪声的理想情况，这种理想情况在实际中是并不存在的，因为再完美的系统你也没办法阻止分子的热运动，除非你想颠覆热力学定理。热噪声或者说高斯白噪声总是如影随形，无处不在的。

在没有噪声的情况下，数据率的限制仅仅来自于信号的带宽。那么奈奎斯特带宽的就可以如下描述：如果带宽为 B，那么可被传输的最大信号速率就是 $2B$；反过来说如果信号传输速率为 $2B$，那么频宽为 B 的带宽就完全能够达到此信号的传输速率。这一限制来自码间干扰，有着严格的数学证明，对相关证明感兴趣的读者可以参见参考文献 5 的第 9 章。

也就是说，对于 GSM 这样的 200kHz 的频点带宽，其奈奎斯特带宽的最大传输速率可达 400kbit/s（这很理想化），而实际的传输速率为 270.833kbit/s。

2.7.2　有噪声的真实信道——香农容量

奈奎斯特准则指出，在无噪声的完美信道里，带宽加倍则数据率或者说信道容量也加倍，在没有噪声干扰的前提下，这样的结论的确合情合理。实际上的信道则比这要复杂得多，高斯白噪声（热噪声）、突发噪声、衰减失真都会对信道上传输的信号产生影响，造成信号丢失或者误码等。

在有噪声的情况下，带宽增加就不一定能相应地增加传输速率了，因为带宽越高，由于频带的展宽，相应的高斯白噪声也会增多，对数据的影响也就会相应地增加。

对于一个给定的噪声电平，我们希望通过提高信号强度来提高正确接收数据的能力。在这里，用信噪比（SNR，Signal-to-Noise Ratio）来衡量信号功率相对噪声功率的强度，这个值越大，说明信号越好，我们越容易分辨出信号来。SNR 为信道输出的信号功率 S 和输出高斯白噪声功率 N 的比值，即 $SNR=S/N$。

对于数字传输而言，带宽和信噪比共同决定了一个信道的容量，可以用一个简单的公式来描述，这个公式是由香农推理出来的，这就是著名的香农定理：

$$C = B\,\mathrm{lb}\left(1+\frac{S}{N}\right)$$

由于高斯白噪声的功率 N 与信道带宽 B 有关，若噪声的功率谱密度为 n_0，则功率噪声 N 将等于 n_0B。因此，我们可以将香农公式转化为

$$C = B\,\mathrm{lb}\left(1+\frac{S}{n_0 B}\right)$$

从这个关系式就可以清楚地看出，增大带宽 B 不一定就能使 C 不断增加，甚至当 B 趋近无穷大时，C 是一个给定的有限值，对此可以给出数学上的证明。

$$C = B\,\mathrm{lb}\left(1+\frac{S}{n_0 B}\right) = \frac{S}{n_0}\cdot\frac{n_0 B}{S}\mathrm{lb}\left(1+\frac{S}{n_0 B}\right)$$

当 $B\to\infty$ 时，则上式变为

$$\lim_{B\to\infty} C = \lim_{B\to\infty}\left[\frac{n_0 B}{S}\mathrm{lb}\left(1+\frac{S}{n_0 B}\right)\right]\left(\frac{S}{n_0}\right) = \mathrm{lb}\,\mathrm{e}\left(\frac{S}{n_0}\right) \approx 1.44\frac{S}{n_0}$$

由此可见，当 $\frac{S}{n_0}$ 保持一定时，即使信道带宽 $B\to\infty$，信道容量 C 也是有限的，这是因为信道带宽 $B\to\infty$ 时，噪声功率 N 也趋于无穷大。

香农定理指出了达到一个既定信道的最大容量，却没有提及如何去实现它，所以香农容量暂时只是一个衡量实际通信系统性能的尺度。

另外，上述关于信道噪声的讨论都是以高斯白噪声为前提的，对于其他类型的噪声，香农公式需要加以修正才能适用于实际的情况。

2.8 无线信道的衰落

有线信道相比无线信道而言是比较简单的，以同轴电缆为例，它内部用金属传输信号，外部用塑料进行绝缘，信号就在里面传输，四平八稳，其物理特性自出厂起就是恒定的。我们通常也称有线信道为恒参信道，也就是说各项参数是不变的。

而无线信道就大不相同了，无线信道的物理特性没有一刻是恒定的，总是处于不断变化中，也称作变参信道。对于无线信道而言，最要命的特性莫过于衰落（fading）现象：由于多径效应引起的小尺度效应，以及由距离衰减引起的路径损耗或者障碍物造成的阴影等大尺度效应。

2.8.1 大尺度效应

所谓大尺度效应，也称大尺度衰落或者慢衰落，是比较好理解的一种，因为我们很容易找出直观的东西来和它类比，那就是光波，请记住了，光波也是电磁波，只不过是频率不同的电磁波而已，所以有很多东西是比较类似的。

电磁波的电场会因为距离而衰减是显然易见的，光波也是如此，一束手电筒的光照向夜空，要不了多远就基本看不到了。一是因为电磁波在空中四散传播，发散了，另一



点是因为路径造成了能量的损耗，在无线通信中也有类似的效果。

因为路径造成的场强的损耗遵循自由空间传播模型。什么叫自由空间传播模型？它是做什么用的？自由空间传播模型一般用于预测接收机和发射机之间完全无阻挡的视距路径时接收信号的场强，比如卫星通信系统和微波视距无线链路就是典型的自由空间传播。自由空间中距发射机 d 处天线的接收功率由 Friis 公式给出：

$$P_r(d)=\frac{P_tG_tG_r\lambda^2}{(4\pi)^2d^2L}$$

式中，P_t 为发射功率；$P_r(d)$ 为接收功率；G_t 是发射天线增益；G_r 是接收天线增益；d 是发射机与接收机之间的距离，单位为 m；L 是与传播无关的系统损耗因子（$L \geqslant 1$）；λ 为波长，单位为 m。其中天线的增益与天线的有效截面 A_e 相关，即

$$G=\frac{4\pi A_e}{\lambda^2}$$

由自由空间公式可知，接收机功率随发射机与接收机距离的平方而衰减，即接收功率衰减与距离的关系为 20dB/10 倍程。

上面我们讲的就是路径传播损耗，它反映出传播在宏观大范围（千米量级）的空间距离上的接收信号电平平均值的变化趋势。路径损耗在有线通信中也存在。下面介绍另一种大尺度效应，那就是阴影效应。它主要是指电磁波在传播路径上受到建筑物等的阻挡而产生的损耗，它反映了在中等范围内（数百波长量级）的接收信号电平平均值起伏变化的趋势。这类损耗一般为无线传播所特有。它服从对数正态分布，其变化率比传送信息率慢，故称为慢衰落。阴影效应在光波里也有，比如你拿一张纸遮住日光灯的灯光，那么从纸背面透过来的灯光就明显弱了很多。

由上可以看出，所谓的大尺度和小尺度，是按照波长来进行划分的。

2.8.2　小尺度效应

小尺度效应又称小尺度衰落、快衰落。它反映了移动台在极小范围内（数十波长以下量级）移动时接收电平平均值的起伏变化趋势。当接收机移动距离与波长相当时，其接收功率可以发生 3 个或 4 个数量级（30dB 或 40dB）的变化。

小尺度效应一般是由多径传播引起的。所谓多径传播，指的是同一传输信号沿两个或多个路径传播，以微小的时间差到达接收机的信号相互干扰。快衰落包含许多类型，如果想要详细了解，请参见参考文献 6 的第 5 章。在这里，仅仅举个例子说明小尺度衰落对于无线通信的危害，让大家有一个直观的认识。

图 2.30 所示的快衰落称为瑞森（Rician）衰落，所谓瑞森衰落就是指除了有间接的多径信号以外，还有直接的 LOS 路径（即视距路径），通常瑞森衰落的结果没有图 2.31

那么惨，因为直接路径的信号强度要强于间接路径，不会出现完全抵消的情况。

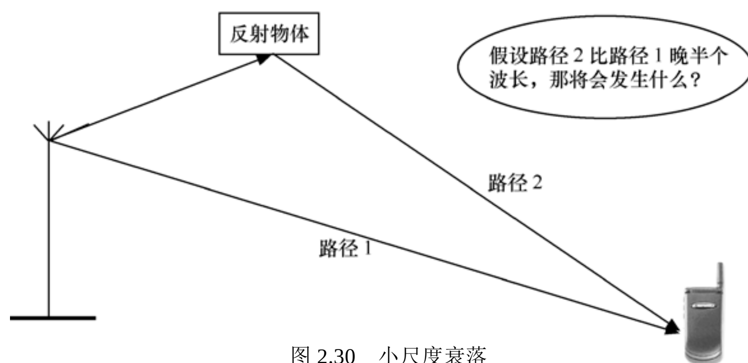


图 2.30　小尺度衰落

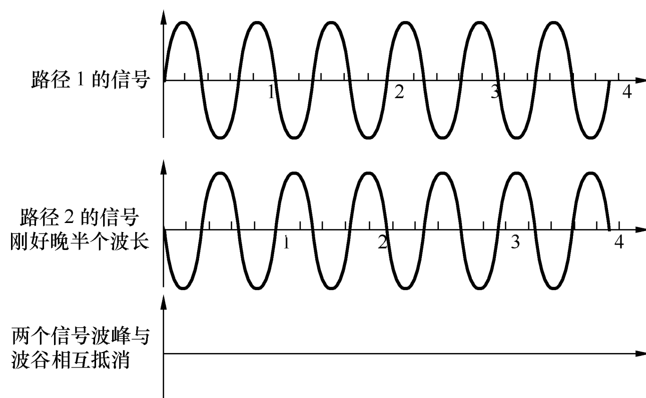
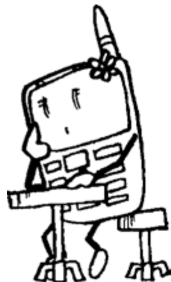


图 2.31　半波长的信号波峰与波谷相互抵消

第 3 章
Chapter 3



GSM 空中接口技术

3.1 稀缺的无线资源及其复用技术

电影《天下无贼》里有一句话很逗却很有道理，那就是黎叔说的："21 世纪什么最贵？人才！"这句话放到无线通信的语境里我们也可以问一句："对于无线通信而言什么最贵？"答曰："空中接口的频率！"

用任何语言来形容空中接口频率的重要性都不为过：不可或缺、无与伦比、至关重要……这样形容夸张吗？一点都不夸张。空中接口的频率对于运营商而言无疑是最重要的战略资源，或许很多人不相信这一点，本节就将对这一问题展开间接的论证。

首先，在中国，无线频谱资源是由政府直接分配给运营商的，所以很多人对无线频谱资源蕴含的巨大价值并不敏感。而在欧洲的很多国家，运营商的频谱资源是通过拍卖获得的，从频频拍出天价你就会发现：这东西的确很贵，很值钱！

其次，如果你深究无线通信系统的技术细节，就会发现，对于无线通信而言，最头疼的问题倒不是大尺度衰落和瑞利衰落。无线通信最头疼的问题是空中接口的频率竟然如此稀缺，以至于不得不设计无数复杂的技术来有效地利用它。

无线通信相对于有线通信而言，最大的区别就在于空中接口。无线通信中种种复杂的技术，几乎都与空中接口有关，空中接口技术在无线通信中的地位，简直可以称得上是"皇冠上的明珠"。而这一切最主要的原因，还是因为空中频率的稀缺性。为了尽可能多地让多个手机利用同一个频段，无线通信设计了多址复用技术，比如空分复用、频分复用、时分复用、码分复用；为了应对多址复用带来的种种干扰问题，GSM 更是绞尽脑汁，想出了功率控制、不连续发射、不连续接收、跳频、设置时间提前量等一系列对抗"多址复用后遗症"的方法；为了榨干每个频点上的最后一滴血，GSM 光在物理层上就设计了 15 种信道，把自己搞得无



比复杂，让俺们每每学到信道这部分内容时就不禁要咬牙切齿：“搞出这么多信道地球人都记不住！”总之，一部无线通信技术发展史，简直就是一部无限的人类智慧与有限的频谱资源进行浴血奋战的斗争史。不过这部历史可没有当年明月的《明朝那些事儿》好读，学通信的俺们往往被搞得焦头烂额。

接下来，就让我们对频率资源及其复用技术进行一番稍微详细的探讨吧。

3.1.1 无价的战略资源——空中接口的频率

无论是军事还是商业，通常都遵循着“克劳塞维茨准则”。在军事上，讲究把最多的兵力放在具有决定性的方向；在商业上，也往往要求把最多的资源配置在具有决定性的方向上。欧洲的电信运营商们在 3G 频段拍卖会上豪掷千金，频频拍出让人瞠目结舌的天价，无疑从一个侧面印证了频率的重要性。

以德国电信为例，为了获得 3G 的 10MHz 频段竟然花了 77 亿美元，每 1MHz 频段价值 7.7 亿美元。7.7 亿美元相当于什么概念，当前的国际黄金价格约为 31 美元每克，7.7 亿美元可以买 24t 黄金。Oh My God，1MHz 频率相当于 24t 黄金，这频率真是比黄金圣斗士还要黄金圣斗士。

我们举这个例子，无非想说明空中接口的频率很贵很值钱，是运营商要去争夺的战略资源。但是我们没有去深究为什么空中接口的频率这么值钱，有线通信中的频率资源是否也这么值钱呢？

空中接口的频率之所以值钱，在于无线通信中电磁波的传播方式和有线通信中的完全不同。无线通信中传递信号的电磁波，如同太阳光一样，是向四周发散传播的，其传播方式在视距的情况下遵循自由空间传播模型，同频率之间信号与信号的干扰不可避免；而有线通信中传递信号的电磁波，却可以控制其传播路径，一条线路上的信号对另一条线路上的信号完全没有干扰。

比如说同轴电缆，几根同轴电缆往往套在一个大的保护套内，如图 3.1 所示。同轴电缆的外保护套是接地的，故外部噪声很少能进入其内部，从而避免了干扰。

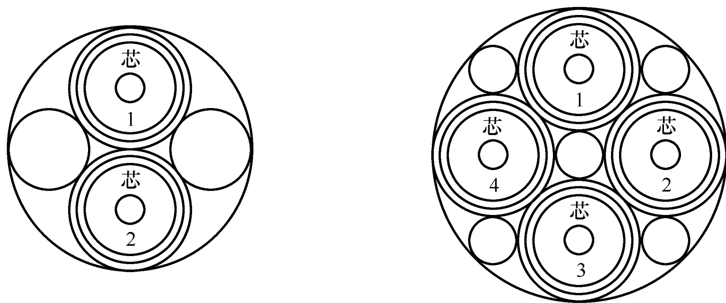


图 3.1 同轴电缆



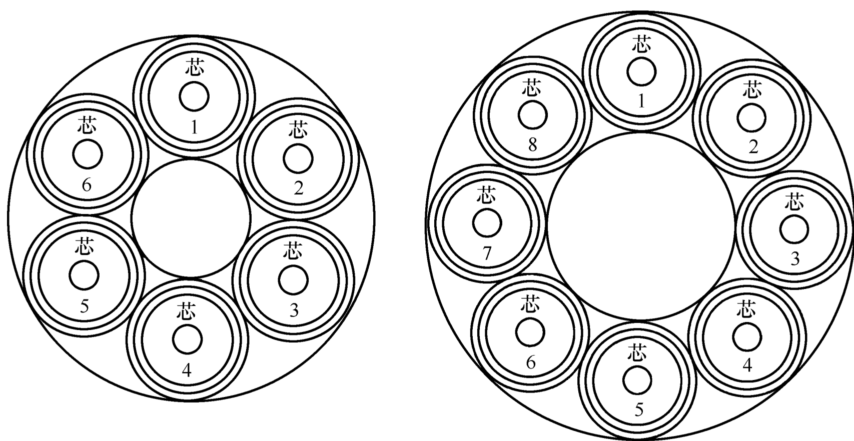


图 3.1 同轴电缆（续）

又比如说光纤，现在大容量高速率的有线通信几乎都以光缆作为载体。如图 3.2 所示，该图为光纤的剖面图，其芯线的直径为 $2a$，包层的直径为 $2b$。芯线的折射指数为 n_1，包层的折射指数为 n_2。

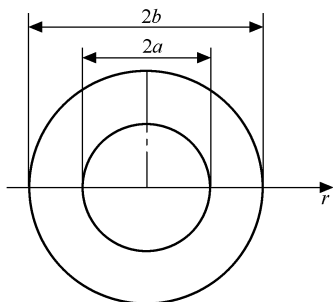


图 3.2 光纤剖面图

对于无线信道，情况比有线信道要复杂得多，我们无法改变电磁波在空气中的传播特性，那么无法有效地控制信号的传播路径，自然也就无法有效地控制同频率信号与信号之间的干扰。既然无法控制干扰，那么我用了这个频段在全国组网运营，你就不能再用这个频段，否则咱俩非得打架不可。频率必须被独占使用决定了它的稀缺性，而稀缺性决定了它的价值，要是它像空气一样谁想用都可以用，那就不值钱了。而在有线通信中则完全没有这个概念，这条线路采用什么频率传递信号与其他线路完全没有关系，谁若异想天开想把固网的频率也搞个拍卖，估计会被笑掉大牙。

注意：空中接口频率的稀缺性对无线通信产生了非常深远的影响。无线通信中的很多技术，包括复用、无线资源管理、功率控制等都是为了尽最大可能有效利用频率资源而设计的。

3.1.2 6MHz 联通 VS 29MHz 移动——工作频段分配

运营商的经营管理常常作为案例被搬上管理学或者营销学的课堂。对于移动和联通的经营，从公司启动时间到市场细分，从定位到战略，从广告宣传到促销手段，从渠道到直

销，都有无数的文章进行详尽的分析。独独缺乏对 GSM 频段划分的分析，其实频段的划分必定会对组网策略产生深远的影响，而组网策略必定会影响运营商的产品战略，进而影响公司的战略定位。所谓的营销策略、传播策略、渠道策略都是战术层面的东西，无不服从和服务于公司的战略定位，因此，频率无疑是公司战略层面上最重要的一环，900MHz 与 1 800MHz 给一个公司所能带来的东西是完全不同的，6MHz 与 29MHz 也是如此。

就技术层面而言，我们并不需要去深究上述问题，本书也不打算就此展开阐述。但是如果我们的目光能更深邃一点，看得更深更远一点，对我们并没有坏处。我们起码可以知道，为什么和记黄埔、T-Mobile、Britain Telecom、Vodafen、NTT、DoCoMo 这些国际巨头都如此舍得在频率资源上花大价钱。

在中国，目前只有 GSM900 和 GSM1800 频段被分配，因此我们只对这两个频段加以阐述。GSM900 的频段上行链路为 890～915MHz，下行链路为 935～960MHz，上下行各 25MHz。GSM1800 的频段上行链路为 1 710～1 785MHz，下行链路为 1 805～1 880MHz，上下行各 75MHz。另外还有一个 GSM 的扩展频段，称为 EGSM（Extend GSM），频率是这样分配的，上行链路为 880～890MHz，下行链路为 925～935MHz，上下行各 10MHz，目前在中国是分配给了中国移动。GSM1800 频段比 GSM900 频段的频率资源要丰富得多，不过由于 1 800MHz 频段电磁波穿透墙体或是其他障碍物造成的路径损耗远远大于 900MHz，1 800MHz 在运营商那里远不如 900MHz 受欢迎。目前 CDMA 所使用的 800MHz 频段和 GSM 使用的 900MHz 频段是公认的通话的“黄金频段”，也是运营商争夺的焦点。

GSM 目前采用的载频间隔为 200kHz，也就是 1MHz 带宽可分为 5 个频点，那么 GSM900 一共有 25×5−1=124 个频点，GSM1800 一共有 75×5−1=374 个频点。

GSM900 的标称中心频率与序号的关系由以下公式确定：

$$上行频率\ f(n)=890+0.2n(\text{MHz})$$

$$下行频率\ f(n)=935+0.2n(\text{MHz})$$

式中，n 为绝对频率号，范围为 1～124。

通常情况下，我们说的上行频率的 1 号频点就是指中心频率为 890.02MHz、频宽为 200kHz 的频段。那么 95 号频点就是 f（95）=890+（0.2×95）MHz=909MHz。在中国，95 号频点一般是闲置不用的，是作为运营商与运营商之间的保护频带。

GSM1800 的标称中心频率与序号的关系由以下公式确定：

$$上行频率\ f(n)=1\ 710+0.2\times(n-511)(\text{MHz})$$

$$下行频率\ f(n)=1\ 805+0.2\times(n-511)(\text{MHz})$$

式中，n 为绝对频率号，范围为 512～885。

目前中国的频段是这样分配的，在 GSM900 上，中国移动占用 890～909MHz 上行，935～954MHz 下行，即 1～94 号频点，另加 EGSM 的 10MHz 频谱；中国联通占用 909～



915MHz 上行，954～960MHz 下行，即 96～124 号频点。在 GSM1800 上，中国移动占用 1 710～1 720MHz 上行，1 805～1 815MHz 下行，即 512～562 号频点；中国联通占用 1745～1755MHz 上行，1840～1850MHz 下行，即 686～735 号频点。

或许又有人要问，这个频率有这么金贵吗，GSM900 不过占用了 890～915MHz 上行，935～960MHz 下行。我再搞个 GSM600、GSM700 甚至 GSM450 频段就可以了嘛，问题就解决了。

呵呵，这个问题我们也希望如此，这样一来问题就简单了。但频率的分配不是俺们说了算，得国际电信联盟（ITU）说了才算，从交通到电力，从微波电视到集群通信，要用到无线方式通信的行业多了去了，想得到新的适合无线通信的频段是非常困难的。

3.1.3　从大课堂到小课堂——空分复用与蜂窝

前面我们说过了空中接口的频率资源非常珍贵，那么如何利用好这些频率显然是一个很重要的课题。显然，我们希望在分配的有限的频段里面支持尽量多的用户。我们知道，频率之所以珍贵，源自它的稀缺性，它的稀缺性源自同频率的信号会互相干扰。那么我们要提高频谱资源的利用率，要解决的就是干扰问题。解决干扰问题的方法有很多，途径之一就是通过“空分复用（SDM）”。

作者记得刚刚上大学的时候，是在一个很大的梯形教室上课，哗啦啦的好几百人在讲台下面。老师讲课的时候有一个扩音话筒和音箱，感觉跟听广播差不多。这种授课方式很快就被证明了不适合教学，因为教学是双向的，只有教师授课这条前向链路是不行的，学生有疑问是要发问的，必须要有可以发问的反向链路。然而在这种大教室模式下，学生你一言我一语，搞得整个教室喧嚣无比，咱说话的频率都是 20～3 400Hz 这个区间，谁还不能干扰谁啊。眼看这种广覆盖模式的教学搞不成了，学校采取了小教室授课的模式，你们这些学生说话的频率不就在那个区间，人多了就会互相干扰吗，那好，咱从空间上把你们隔开了，咱学校不过是多几个老师，能教的学生就增加了，用通信的术语说，容量就增大了。

早期的移动通信与这也有点类似，20 世纪 70 年代在纽约建立了贝尔移动系统。这个系统建在高塔上，用大功率的发射机来获得一个广覆盖，最广可以覆盖 2 800km^2。但是很遗憾，它只有 12 个频道，只能支持 12 个用户同时通话。

一个基站可以覆盖这么大的区域无疑是令人羡慕的，按这种效率，几千个基站就能实现美国境内的全覆盖。但是如此大的覆盖范围带来的问题比惊喜更多。只能支持 12 个用户，那么这个系统能做什么用呢？用于军事，算了吧，我还不如用电台呢。贝尔移动系统要商业化，要赚钱，当然希望容纳尽量多的用户。

贝尔移动系统首先想到的是希望从政府那里获得更多的频谱资源。政府当然不干，



频谱资源多宝贵啊，无绳电话不要用啊，集群通信不要用啊，公共交通不要用啊，微波电视不要用啊，卫星通信不要用啊……总之，俺这里的频段都有主了，没有主的也是为了未来而准备的，你总不能把子孙后代的资源也占掉吧，你自己想办法去，爱干嘛干嘛，爱谁谁，总之别打我这里的主意。

贝尔移动系统碰了一鼻子灰，甚是郁闷，不得不从自身想办法。一个靠谱的主意是把发射机的功率做小，然后增加基站的个数。这样，虽然分配的频谱段没有增加，但是系统能容纳的用户增多了，如图 3.3 所示。

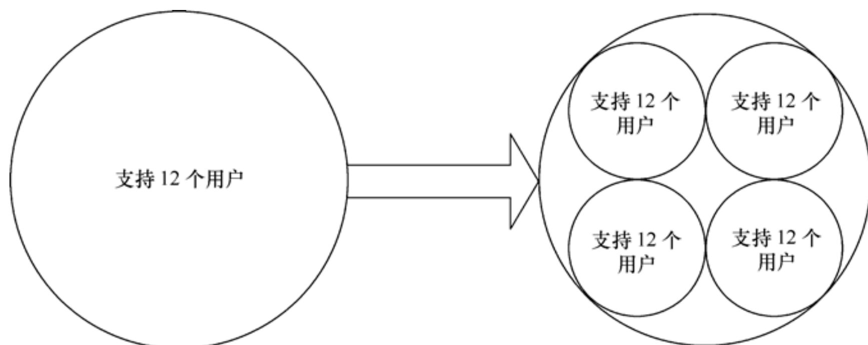


图 3.3　增加系统容量的方法

图 3.3 中假设基站处于圆心，圆形覆盖的区域即基站的覆盖半径。这仅仅是一个基本的思路，在实际应用过程中，不会像我们画图这样完美，电磁波在空中要经过衍射、散射和反射，实际形成的传播路径和传播范围是十分复杂和不规则的，不会像画图一样是个圆形，另外基站和基站之间也不可能如图 3.3 所示组成一个个等距的圆形。实际上基站与基站之间会有大量重叠覆盖的区域，在这些区域里，同样频率的信号是个问题，它们一样会互相干扰，一样会降低系统的容量。实际覆盖情况示意图如图 3.4 所示。

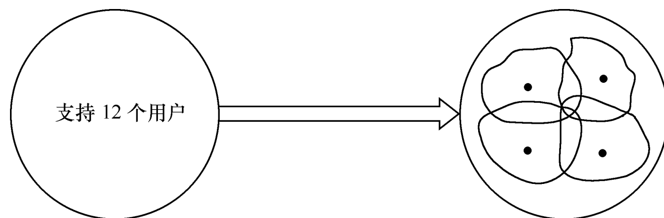


图 3.4　基站实际覆盖效果图

在降低发射机功率以控制覆盖范围之后，设计者又开始从天线上做文章。我们知道，早期的天线是全向天线，其电磁波是向四面八方均匀发射的，如图 3.5 所示。

图 3.5 所示的全向覆盖的方式在基站的实际覆盖上显然会遇到问题，12 个频段都用



上的话，在交叉覆盖的地方信号会干扰得一塌糊涂。于是，我们希望信号可以使用定向波束来覆盖，于是就产生了扇形定向天线，如图 3.6 所示。

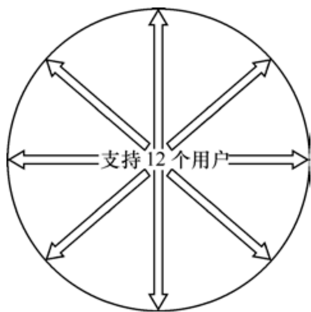


图 3.5　全向天线的电磁传播

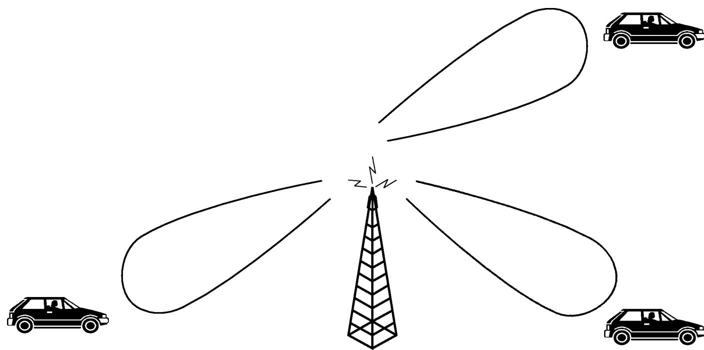


图 3.6　定向天线的应用

采用定向天线后，我们就可以控制将不同频率的信号通过不同的天线定向发射到某一方向，从而避免在信号重叠区域的干扰。定向天线也是蜂窝通信中非常重要的组成部分。

这就是蜂窝通信的理念，当希望增加更多用户时，就进行小区分裂，把一个大的小区划分为很多小的小区，同时降低发射机的发射功率，以减小单个发射机的覆盖范围，尽量避免同频干扰，从而可以通过发射机数量的增加来服务于更多用户。

总结：所谓复用技术，指的就是区分在同一频段下通信的不同终端的技术，系统必须能有效区隔各终端才能完成通信。空分复用是从空间上将使用同一频率的不同终端区隔开来；频分是把一个频段分为若干块，不同的终端占用不同块；时分复用是从时间上将终端区隔开来，不同的终端通过占用不同的时间块来实现区分；码分复用是通过终端占用的不同的扩频码来区分。

3.1.4　也谈广电架构与电信架构的异同——频分复用与时分复用

空分复用是提高频谱利用率的有效方法，不过这还不够，我们需要继续探索其他复用技术，提高频谱利用率，以满足无线通信的迅猛发展。本节就探讨一下复用技术的另外两种方式——频分复用（FDM，Frequency Division Multiplexing）和时分复用（TDM，Time Division Multiplexing）。

1. 频分复用（FDM）

所谓频分复用，其实并不新鲜，在广电的架构下就有这种技术。以前我们的电视信



号是通过微波传输的，如今是通过有线同轴电缆进行传输的，不管哪种传输方式，并没有改变不同的电视台使用频分复用进行区分的实质。我们看电视的时候经常调换频道，对频道这个概念想必已经非常熟悉。所谓频道，指的就是频率段，不同的电视台占用不同的频率段，以和其他电视台进行区别，这就称为频分复用，比如 CCTV1～CCTV8 就是一个典型的频分复用系统。

如果说以电视打比方还显得有点模糊的话，那么用同属广电系的广播打比方就要亲切多了。因为电视并不自报家门告诉你它用的哪个频段，而广播则不一样，当你收听广播的时候，广播电台总要无数次地把它所使用的频率告诉你，生怕你下次会遗忘它。比如调频 97.5，湖南音乐频道；调频 98.1，长沙交通频道。它们传送美妙的音乐也好，广播实时的路况信息也罢，总之用的是不同频率的信号，井水不犯河水，不至于互相干扰。

电信系统的架构和广电系统的架构其实有颇多相似之处，我们可以把基站的发射机（或者说载频）理解为一个个的电台，电台与电台之间采用不同的频率，那我们的载频与载频之间也采用不同的频率，这样，就构成了一个无线通信的频分复用系统。

电信系与广电系虽然有很多相通的地方，但是有一个地方是截然不同的。那就是广电的构架是单向的，无论电视也好广播也罢，都是它们向观众或者听众发送信号，没有观众或者听众向电视台或者电台发送信号一说。广电系的频分仅仅是前向链路（下行链路）的频分，它是没有反向链路的，所以也谈不上反向链路的频分。还有一个最大的不同，那就是广电系传递给每一个用户的信号都是一样的，所以它可以以广播的形式向用户传播，一个频道就可以服务于成千上万个用户，因为用户收到的信号没有什么区别。而电信系的用户是在沟通和交流，显然每一个用户的信号都与别的用户不同，所以一个用户必须独占一个频道来实现通信，如果这个频段还有其他用户的信号，那很糟糕，双方会互相干扰。

在 GSM 里面的频分复用是这样实现的，就是把 890～915MHz 这个频段均匀地划分成 124 块，每一块占用 200kHz 的频段，也就是我们常说的频点，一个用户通话的时候就独占一个频点，它周围的用户在这个时刻是不能够占用相同的频点的，要不就会有干扰。

2. 时分复用（TDM）

频分复用和空分复用一起，为俺们的无线通信作出了杰出的贡献。但是还是有一件事令俺们非常郁闷，那就是一个用户通话的时候需要独占一个频点，也就是说一个收发信机（一块载频）就被他一个人霸占了，这令人相当不爽。人类解决问题的智慧总是相通的，面对这个资源独占型难题，俺们不妨也向广电取取经。

在作者所在的 Y 市，YIYTV 要举办一场招商引资的晚会，那可谓人山人海，锣鼓喧天，鞭炮齐鸣，红旗招展……这样的盛况谁不想参加呢，于是导演就郁闷了，一个晚



会总共就那么几首歌，这么多歌手要唱，这猪肉是怎么都分不匀啊。后来不知从哪里来的灵感，这位天才的导演总算想出了一个完美的解决方案，那就是歌分复用（Song Division Multiplexing），把一首歌切成 8 块，8 个人一人唱一句，不就都解决了。

GSM 的时分复用与此也颇为类似。如果把一首歌比作一个 TDMA 帧的话，那么一人唱一首歌就好比一人占用一个时隙（time slot）。我们在前面讲过，所谓复用技术，就是区隔用户的技术，在时分复用里面，使用相同频率的用户是通过在不同的时间（时隙）里工作来区分的。

3.1.5　3G 的基础——码分多址

本小节我们要谈谈 CDMA，CDMA 是美国高通（Qualcomm）公司最先提出来的，并由此获得了大量专利，CDMA 也是目前的 3G 无线通信的一个基础技术。无论是 WCDMA、cdma2000 还是 TD-SCDMA，都绕不开 CDMA。高通公司也因为 CDMA，从一个无名的小公司，一跃成为通信行业最具影响力的企业。人们常说一流的公司做标准，二流的公司做品牌，三流的公司做产品。谈到一流的公司的时候，往往拿高通出来做范例，至于高通征收高额专利费这种经营模式导致 CDMA 产业链的发达程度远远落后于 GSM 产业链，那又是后话了。

CDMA 的英文全称为 Code Division Multiple Access，是码分多址的意思。GSM 是采用频分和时分来对终端进行区分的，CDMA 里没有时分复用，它是依靠不同的扩频码来区分不同的终端。

码分是什么意思呢，在这里可以打一个通俗的比方。我们都在一个屋子里说话，大家的声音也都不小，如果都是用中文说话，那麻烦就大了，你会不断地被与你无关的人说的话所干扰，甚至搞得你无法和你想交流的人进行正常的交流。如果大家所采用的编码方式不同，比如你用中文，张三用英语，李四用意大利语，王五用西班牙语，情况就会要好得多。你的对家用中文作为扩频码和你说话，尽管背景噪声很糟杂，但是你还是可以很好地分辨出他的声音，OK，咱可以正常交流。这时候张三说的英语的声波过来干扰了，你的大脑相当于处理机，它就会这么反应：“对不起，哥们，英语咱一窍不通，您的扩频码咱不认识，咱只当是背景噪声直接过滤了。”

请注意的是，扩频码必须有一个特点，那就是必须正交。正交在数学里的概念就是完完全全不相关，两个信号的乘积在某个区间内积分为零。换句话说，就是你这编码和编码之间要没啥相关性，英语和汉语就适合做扩频码，因为英语和汉语没啥相关性，很容易就可以区分开来。（其实这句话并不完全正确，汉语里有很多舶来品，比如沙发—sofa，好莱坞—Hollywood。）但是湖北话和湖南话做扩频码就不合适了，重叠部分太多了，一起说会干扰得一塌糊涂。

应当注意的是，人对世界的理解是多维的，即使是耳朵对声音的理解也不止一个维度，虽然大家说话的声音都是 20～3 400Hz，但是人们可以通过音色、音调和响度来对声音信号进行区分，甚至可以借助视觉来对对方的话语进行理解，因为人说话的时候往往还有表情。所以即使没有正交，人判断和区分信号也相对容易。而机器只能理解比特信息流，它只能从一个单一的维度去思考，所以它的要求自然比人类要严格得多，如果要进行码分复用，那么它所采用的扩频码之间必须正交，以有效区分。

1. CDMA 中的扩频

说了这么多，那究竟什么是扩频呢？CDMA 系统中为什么要采取扩频呢？又是怎样实现扩频的呢？

前面在讲香农定理的时候我们也提过，传输一定速率的基带数字信号需要占用一定的带宽，通常情况下这个带宽与速率之间差别不大。比如说 GSM 系统，信号速率为 270.8kbit/s，而带宽为 200kHz；又比如说 PHS 系统，信号速率为 384kbit/s，而带宽为 300kHz。而扩频通信与此完全不同，在 CDMA 系统中，速率为 9.6kbit/s 时，带宽达到了 1.25MHz，足足是信号速率的 100 多倍，这是扩频通信独有的特点。由于信号的总功率是一定的，信号占用的带宽增加了，那么信号在带宽上的平均功率就下降了。带宽增加导致平均功率下降的示意图如图 3.7 所示。

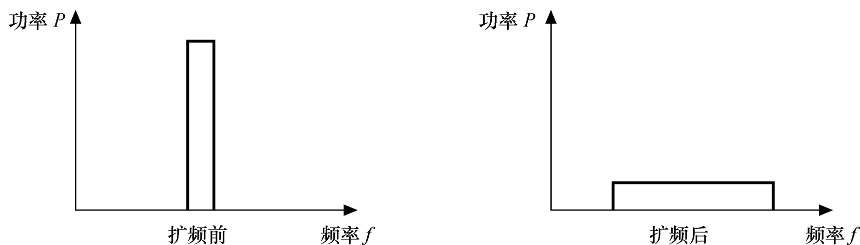


图 3.7　扩频通信

从图 3.7 中可以很明显地看出来，扩频之后，占用的带宽增加了，带宽上的平均功率下降了。上面我们对扩频通信作了一个粗浅的介绍，那么扩频通信的理论基础又源于哪里呢？

扩频通信用上百倍的带宽来传输信号的想法最初看起来有点天外飞仙，因为现代无线通信系统都是尽力压缩单个信号所需的带宽，因为空中接口的频率实在是很有限。比如说 GSM，270.8kbit/s 的传输速率，就只给 200kHz 的带宽，这个带宽甚至都不足以保证邻频之间互相不干扰，所以网络优化中通常都要求邻区不要用邻频。不过没办法，谁让空中接口的频率如此有限呢，您就将就着用吧。

CDMA 中一个 9.6kHz 的语音话路，也要占用 1.25MHz 的带宽，看起来颇让人气愤，



很有点败家子的感觉。不过 CDMA 与 GSM 有一个本质的不同，就是 CDMA 根本就不是频分复用系统，它根本不需要通过不同的频率来区分终端。它是通过不同的扩频码来区分不同的终端的，它之所以要占用 1.25MHz 的带宽就是因为扩频的需要。我们在 3.1.4 节中提到过几种不同的多址接入技术，CDMA 的多址接入技术与 GSM 不同，所以不能拿 GSM 的老眼光来看待它。黑猫白猫，抓到老鼠就是好猫；黑技术白技术，能让更多的用户接入就是好技术，是不是？

虽然这个想法很诡异，但是这个想法也是有理论基础的，那就是香农理论：

$$C=B\ \mathrm{lb}\ (1+S/N)$$

其中 C 代表传输速率，B 代表信道的带宽，S/N 就是信噪比。根据香农定理，在信噪比一定的情况下，信道的带宽越大，传输速率越高；在带宽既定的情况下，信道的信噪比越高，传输速率也越高。信噪比一般由发射机的功率、接收机与发射机之间的距离和噪声信号的强度来决定。

如果信噪比很低（$S/N \ll 1$），香农定理可以简化为：

$$C/B \approx 1.44\ S/N$$

传输同样速率的信号，如果增加信道的带宽，就可以降低接收机信噪比的要求。降低信噪比可以带来很多好处，比如发射机的功率可以降低；或者同样的发射功率，接收机与发射机之间的距离可以增加，从而扩大了基站的覆盖范围。此外，降低接收机信噪比的要求还可以对抗干扰。（这就是为什么 CDMA 最初用于美国军方通信的原因，对抗电磁干扰的能力强啊；电磁干扰的原理一般是对某个频段的信号进行同频干扰，但是 CDMA 不惧同频干扰，因为它本来就是一个自干扰系统。）

由于带宽的增加可以大大降低 S/N 的要求，C 和 B 的比值 C/B 通常被称为处理增益或者扩频增益。

2. CDMA 的抗干扰特性

说了这么多，我想还有很多人对图 3.8 所示圆圈标注部分，也就是空中接口的干扰心有余悸，对 CDMA 如何解决这个问题心里没底，我们不妨进一步说明一下。

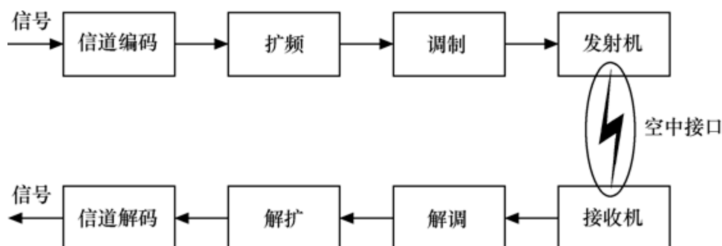


图 3.8　CDMA 的系统框架图

图 3.8 就是 CDMA 的系统框架图，可以看到，与一般的数字通信相比，CDMA 还增加了一个环节，即扩频与解扩。CDMA 是怎样对抗空中接口的干扰的呢，我们先画一个对比图来了解一下（如图 3.9 所示），然后再加以说明。

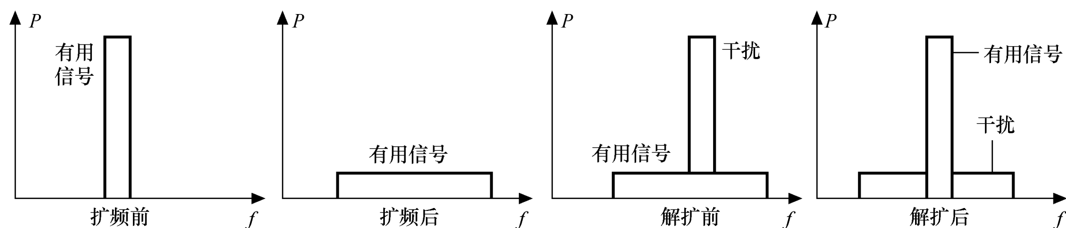


图 3.9　扩频抗干扰示意图

图 3.9 中前两幅图我们已经解释过了，就不再重复。第三幅图，当出现一个窄带干扰时，解扩的过程就相当于对这个窄带信号进行一次扩频，将它的窄带频谱展开为宽带，干扰信号的平均能量被大大降低，对其积分后为零从而过滤掉。

3. 扩频码与扩频码实现的细节

扩频码我们在本节中提得已经够多了，但我们并没有讲扩频码到底是怎样的一串比特信息流，频率展宽到底是如何实现的？

我们打个比方，假设对 1 个信号进行 8 倍扩频（为了画图方便我们姑且这么假设，实际的扩频通信中扩频倍数远不止这个数）。假设比特信息流的数据为“1001011”，调制速率为 R，那么我们把它进行 8 倍扩频，就是拿它的每一个用户数据比特与一个包含 8 个比特的码序列。这样得到扩频后的用户数据，速率为 $8R$，有意思的是，扩频后的用户数据与扩频码有相同的随机特性，这个性质非常重要。

所谓信号的相乘，在二进制里就是基带数字信号与扩频码做模二加得到。模二加是不考虑进位的二进制加法，其结果与二进制异或逻辑运算完全一致，因此也可以用逻辑运算来代替。扩频与解扩如图 3.10 所示，在这里，原始数据是“10”，调制速率为 R，扩频码为“1101100110100011”，调制速率为 $8R$，信号经过一次扩频后数据速率达到 $8R$，解扩后又恢复原来的信号及速率。

到这里，我们或许又要问，随便什么码都可以用来当扩频码么？

如果仅仅着眼于扩频与解扩，那当然什么码型都可以用，反正只要扩频码和解扩码一致就可以把信号恢复出来。可是别忘了我们扩频通信的目的是什么，在这里我们是用在 CDMA 里面的，终端的频率完全相同，要区别终端只能靠扩频码。我们知道，要识别两个不同的物体，自然是这两个物体差别越大越好，这样才不至于混淆。所以扩频码既然是用来识别不同的终端的信号的，那么扩频码与扩频码之间自然是差别越大越好，就



像中文与英文一样，完全不相关才好，在数学里，这个特性叫做“正交”。

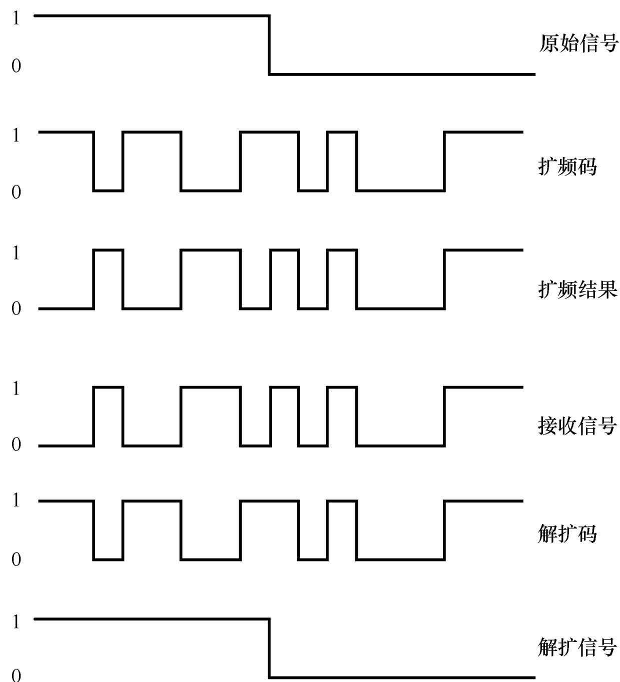


图 3.10　扩频与解扩

在 CDMA（IS-95）里，通常采用的是 Walsh 码和 m 序列，下面我们对 Walsh 码进行介绍。CDMA 里面的 Walsh 码是 64bit 的，我们只介绍 8bit 的，因为通过矩阵运算由 8bit 生成 64bit Walsh 码是很简单的，所以为了方便起见，我们仅对 8bit 的作介绍，如表 3.1 所示。

表 3.1　8bit Walsh 码

编　号	序　列
0	00000000
1	01010101
2	00110011
3	01100110
4	00001111
5	01011010
6	00111100
7	01101001

Walsh 码来自 Walsh 函数，Walsh 函数的取值为+1 或者−1，为了方便表达，可以将+1 和−1 转换为二进制的 0 和 1。我们注意到一个特点，Walsh 码除 W0 外，其余码型中的 0 和 1 数量都相等，这个特性非常有用。Walsh 码具有正交性和归一性。

所谓正交性，指的就是两个码相乘后积分为 0。比如 W1 和 W3 相乘（模二加）的结果是“00110011”，由于二进制的 0 和 1 分别代表+1 和−1，因此累加（离散序列的积分相当于累加）的结果为 0，这就验证了 Walsh 码的正交性。累加更简单的办法是比较 0 和 1 的个数，如果相等，说明累加的结果为 0。

W3 和 W3 相乘（模二加）的结果是“00000000”，累加的结果是+8，平均值为+1，这就验证了 Walsh 函数的归一性。

正交性的特点对于抗干扰非常重要，假如一个手机以 W1 作为扩频码，把信号“10”扩频后发送出去，去干扰扩频码为 W3 的手机，经过扩频和解扩，我们看看会发生什么。

从图 3.11 中我们可以看到，以 W1 作为扩频码的手机，它的原始信号可以被自己的接收方正确地解出。它的信号扩频后在空中接口发送，由于 CDMA 手机占用的频率都是一样的，它的信号也可能被其他手机接收，比如被扩频码为 W3 的手机接收。接收了不要紧，我们从图 3.11 中可以看到，扩频码为 W3 的手机无法还原来自 W1 手机的窄带的

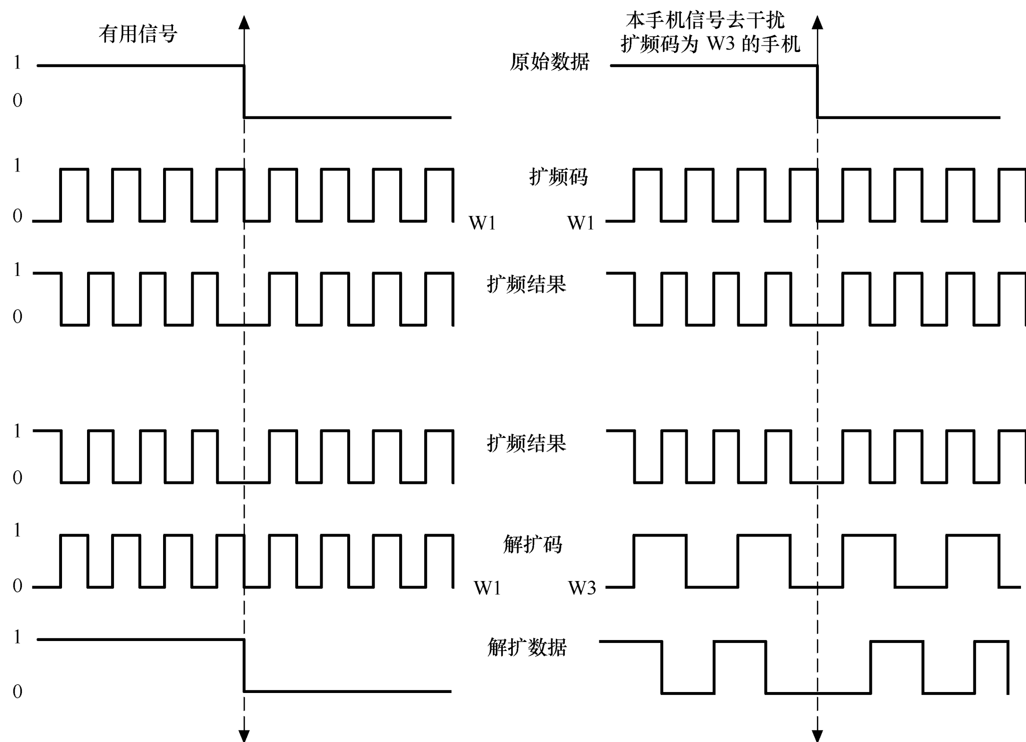


图 3.11　扩频中应对干扰



原始信号，解扩后依然为宽带信号，我们对每个 Walsh 码的 8bit 区间做积分，每个积分区间结果都为 0，就这样可以过滤掉干扰信号。

我们刚刚是举例证明只要扩频码不同，手机就可以有效过滤掉来自其他手机的干扰信号。下面我们要证明这个例子具有普遍意义，首先在逻辑电路里有这么一个结论，信号的异或满足交换律和结合律，那么有：

原始信号⊕扩频码 W_a⊕扩频码 W_b=原始信号⊕（扩频码 W_a⊕扩频码 W_b）

我们知道,（扩频码 W_a⊕扩频码 W_b）两个 Walsh 码相乘满足正交性，即做模二加（不进位的二进制加法）后 0 和 1 的个数相等。

而原始信号与具有正交性的码做异或后不会改变 0 和 1 数目相等的情况，就好比（aaaaaaaa）⊕（01010101），无论 a 取 0 还是 1，对 0 和 1 数目相等的事实没有影响，如图 3.12 所示。

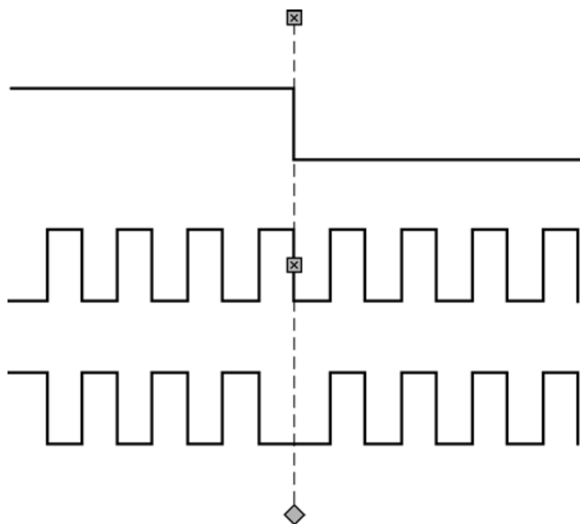


图 3.12 原始信号的模二加

由此我们可以看出扩频码和扩频码之间的正交性这个性质非常重要，我们可以借助这个性质来滤掉来自其他 CDMA 手机的干扰信号，从而实现码分复用。

3.1.6 游走在功率与频率之间——载干比与频宽

根据香农定理 $C=B\,\mathrm{lb}(1+S/N)$，我们知道，要达到一定的传输速率，要么就要在信噪比 S/N 上做文章，要么就要通过增加带宽 B 来实现。信噪比和带宽是无线通信对信道描述的两个维度，无线通信就在这两个标准之间找平衡，如果你希望尽量节省空中接口的频率，那你的信噪比就必须要高，GSM 通常就采用这种方式；如果你打算用带宽来换信



噪比，以使你的发射功率可以做得很低，甚至可以淹没在高斯白噪声中以不被人发现，那么你就去扩频好了，CDMA 通常就采用扩频来以带宽换信噪比。

1. GSM

我们知道，在 GSM 里面，频率是要复用的。在给定的同频再用距离上，某小区将使用其他小区也在使用的信道。这意味着该小区将受到来自使用相同频率的信道小区的干扰，最终基站的覆盖范围将受到频率干扰所限制。相对于传统的噪声受限系统而言，成熟的蜂窝系统是干扰受限的，干扰才是最大的问题。

在无线通信中，通常用载干比来衡量干扰。在 GSM 中，通常需要考虑同频干扰（C/I）和邻频干扰（C/A）。

所谓同频干扰，是指当不同小区使用相同频率时，另一小区对当前服务小区所产生的干扰，它们的比值即 C/I。GSM 规范中通常要求 C/I>9dB；工程中为了稳妥起见，一般加 3dB 的余量。

所谓邻频干扰，是指在频率再用模式下，相邻频率会对服务小区所使用的频率进行干扰，这两个信号间的比值即 C/A。邻频的信号比当前所占用的频点功率高没关系，只要不是高得太多就行。GSM 规范中一般要求 C/A>−9dB，工程中一般也加 3dB 的余量，即要求 C/A>−6dB。

应对同频干扰和邻频干扰的载干比要求是计算机仿真和工程实地勘察得出的结果，我们对此不加深究。

除了同频干扰和邻频干扰，载波偏离 400kHz 的时候也可以产生干扰，不过实在非常罕见，除非干扰信号的电平远远高于当前载波电平。GSM 规范中要求载波偏离 400kHz 时的干扰保护比 C/A>−41dB，工程中一般加 3dB 的余量，即 C/A>−38dB。

我们在前面提过，GSM 的频道间隔是 200kHz，实际上，200kHz 的带宽对于 GSM 而言并不足够，所以工程上一般要求邻小区不能使用邻频。频道间隔划成 200kHz 算是在商业和技术之间寻找的一种平衡吧，因为空口的资源实在很珍贵。

2. CDMA

CDMA 的运作思路和 GSM 完全不同。CDMA 由于是靠扩频码来区分不同终端，而且扩频码之间具有正交的特性，使得 CDMA 完全不惧同频干扰，可以同频组网。

我们在前面提过，当 $S/N \gg 1$时，香农公式可以简化为 $C/B=1.44S/N$。CDMA 就用扩频的方式，你只要传输 9.6kbit/s 的数据，我也给你 1.25MHz 带宽（扩频的码片速率 1.228 8Mchip/s，加一点保护带宽）。这样，C/B 的值就变得很小，从而信噪比也可以很小。在 GSM 中，高质量的语音连接所需要的 C/I 的值为 9～12 dB，而在 CDMA 中，通



常为−10～−15dB。而在 WCDMA 中，由于码片速率更高，带宽更宽，信号功率比干扰或者热噪声低 20dB 也照样可以检测出信号来，也就是说，−20dB 也是可能的。

我们要注意的是，对于无线通信而言，扩频和解频操作本身并不能提供任何的信号增强。信号的增强是以增加传输带宽为代价得来的。

3.2 如何应对无线信道的以下挑战：多径效应及瑞利衰落

多径效应和瑞利衰落对于无线通信而言是一个巨大的挑战，尤其是对于 GSM 这样一个时分复用系统来说。为了应对瑞利衰落，GSM 采用了一系列的技术手段，比如信道编码（增加信息的冗余度）、交织技术（时间分集，用于克服信道编码不能还原长串信息丢失的弱点）、跳频技术（频率分集，降低瑞利衰落发送的可能性，以及将干扰平均化）；为了应对多径效应带来的时间色散问题，GSM 设计了训练序列和自适应均衡器，以保证可以测算无线信道的特点，从而对接收机的一些参数进行校正以保证最好的接收效果；最后，因为 GSM 系统是个严格的 TDMA 系统，为了避免时隙和时隙间互相干扰，因此手机发射的时候必须根据到基站的远近加一个时间提前量 TA（Time Advance）值，确保基站接收时不会因为在空中传播的时延而不能准确地在属于自己的时隙发射和接收，从而影响到别的时隙。

本节就将对这些问题一一进行介绍。

3.2.1 当老师的艺术——语音编码与信道编码

语音编码其实与多径效应以及瑞利衰落半点关系也没有，但是在传统的经典的无线通信中，信源编码和信道编码总是放在一起进行阐述的。因此，本节也采用这样的结构，现在开始有一种潮流，即联合编码，也就是不区分信源编码和信道编码，而采用统一的综合的编码。这样做起来并不容易，因为信源编码和信道编码要考虑的问题是完全不同的，信源编码要考虑的是减少冗余度的问题，也就是不要讲废话，尽量要精炼；而信道编码要考虑的是在一个处处是噪声的嘈杂环境中，你的话不断被噪声打断，但你依然要让对方听得明白的问题。

1. 语音编码

我们在第 2 章中已经对编码问题进行过阐述，因此本节只对 GSM 的编码进行介绍。GSM 系统语音编码采取了混合编码，即速率为 13kbit/s 的 RPE-LTP（规则脉冲激励-长期预测）。

因此参数编码器首先将语音分成 20ms 为单位的语音块，再将每个块用 8kHz 进行采样（第 2 章提到了，人耳敏感的语音频率一般为 20～3 400Hz，按照奈奎斯特定理，用二倍频采样，所以用 8kHz），我们可以得出 8 000Hz/s×0.02s=160 个样本。然后每个样本再经过 A 律 13bit（μ率 14bit）的量化。GSM 系统定位的是全球通信系统，它如果想漫游，必须综合考虑到欧洲（A 律）和美国（μ律）标准不一的情况，所以它在 A 律后加了 3bit，μ律后加了 2bit，那么采样后就形成了 16bit。

我们粗粗一算就知道这个结果直接拿来用而不经过信源编码会有多么恐怖，16bit/样本×160 样本×(1s/20ms)=128kbit/s。我的天啊，按这样的编码方式每时隙的空中接口速率将要达到 128kbit/s，这显然是不可接受的，我们需要压缩，再压缩！

语音有一个好处，虽然你听到的每句话和每句话之间是不同的，但是对于 20ms 和紧接着的 20ms 这么短的时间而言，它的变化是极小的，这就给我们带来了操作的空间。

GSM 里面采用了 LPC（线性预测编码）、LTP（长期预测）和 RPE（规则脉冲激励）为波形编码器，编码结果再通过复用器混合完成语音信号的编码。编码器模仿了人类发音器官的组合，其工作原理是将该组合看成一个滤波器，人类发出的声音相当于激励脉冲。当然滤波器的参数一直在变，但从很短的时间（比如 10～30ms）来看它，则基本不变。

这些编码器的具体工作细节我们不再细究，要知道的是，经过语音编码的压缩后，每 20ms 的比特为 260bit，那么可以采用上面类似的方法得出其数据率是 13kbit/s。我们知道，Abis 口和 A 口之间每时隙的速率为 16kbit/s。为了便于在 Abis 口和 A 口上传送，我们通常给它再增加一个 3kbit/s 的信令。

2. 信道编码

信道编码其本质就是通过增加信息的冗余度来实现对信息的保护，其代价是增加了开销，降低了信息量。

我们可以这样打一个比方。语音编码就是上课的时候老师教你的知识，字字珠玑，货真价实。老师想在尽量短的时间内教你尽量多的知识，自然要简洁、凝练。而信道编码就是老师课后给你布置的习题，光凭课堂听讲，你能保证老师讲的自己都听到了吗，都能理解而不会遗忘吗？从纯理想的情况来看，课后习题似乎是没有必要的，它就是对课堂信息的冗余，甚至我们花在课后习题上的时间一点也不比上课少，好像很浪费。但通常情况下，你必须用它来校正自己对课堂上老师教的知识的认识是否全面、是否有误，这与信道编码的作用颇为相似。

我们在语音编码之后，产生了 260bit/20ms 的原始数据，换算起来就是 13kbit/s 的编码速率。而我们需要在原始数据上附加一些冗余比特信息，增加的这些比特是通过某种



约定从原始数据中经计算产生的，接收端的解码过程利用这些冗余度比特来检测误码并尽可能纠正误码。如果收到的数据经过同样的计算所得的冗余比特同收到的不一样，我们就可以确定信息有误。

我们也可以这样理解，老师教完知识以后，就给我们一堆习题，这些习题都是从知识点衍生出来的。老师教课的时候，有些信息可能被我们遗漏了，有些可能理解有误，也就是说你这个接收机接收的信号和你的老师这个“发射机”发射的信号可能并不完全一致。我们拿到习题一算，然后和答案一比对，哦，这个不对，这个我的理解错了，需要校正一下。

GSM 使用的编码方式主要有块卷积码、纠错循环码和奇偶码。块卷积码主要用于纠错，当解调器采用最大似然估计方法时，可以产生十分有效的纠错结果。纠错循环码主要用于检测和纠正成组出现的误码，通常和块卷积码混合使用。奇偶码则是一种普遍使用的最简单的检测误码的方法。

3. 全速率 TCH 信道编码

在对全速率语音编码时，我们并不对 260bit 一视同仁，而是有所区别对待。我们将 260bit 分成 3 类，分别为 50 个最重要的比特、132 个重要比特以及 78 个不重要的比特，划分的原则是根据编码器的高位和低位进行的，这里我们就不展开了。

我们首先把这最重要的 50bit 加上 3bit 的奇偶校验位，这 53bit 然后连同 132 个重要比特与 4 个尾比特一起进行 1∶2 卷积编码 [(53+132+4)×2=378] 就得到了 378bit，另外 78bit 不予以保护，就得到了 378+78=456(bit)。每 20ms 发送 456bit，那么我们可以得出 456bit×(1s/20ms)=22.8kbit/s。

提示： 很多人容易把语音编码的速率和语音在空中接口发送的速率混淆，本节中我们可以看到，语音编码后的速率为 13kbit/s，语音编码后还要进行信道编码，因此语音在空中接口的发送速率为 22.8kbit/s。语音编码在基站侧还原以后，考虑到 Abis 接口和 A 接口的传输特点，给它加上了 3kbit/s 的信令，因此，语音编码在 Abis 接口的传输速率为 16kbit/s。

（1）LAPDm 帧的编码

我们知道，LAPDm 是空中接口的数据链路层的协议，在连接模式下被用于传送信令。它被应用在逻辑信道 BCCH、PCH、AGCH、SDCCH、FACCH、SACCH 上。我们发现， SCH 和 RACH 并不算在 LAPDm 帧里边，道理也很简单，SCH 以及 RACH 并不像上述的信道一样采取的是普通突发脉冲，其脉冲形式有所不同。

一个 LAPDm 帧共有 23Byte，即 184bit，为了和突发脉冲相适应，我们也需要像 TCH 信道一样生成 456bit。首先给这 184bit 增加 40bit 的纠错循环码，这样就可以来检测是否物

理层的差错校正码能正确地校正传输差错。通过这种码型来检测无线链路，来确认 SACCH 消息是否被正确地接收到。检测的具体方式，我们会在后面的无线链路故障一节里提到。

为了实现卷积编码，还要增加 4bit 的尾位。这样我们就得到了 228bit，经过 1∶2 卷积后，就得到了 456bit。456bit 放到 4 个突发脉冲里，每个突发脉冲为 114bit。在此我们需要做一个解释。虽然一个突发脉冲序列有 156.25bit，但它只能携带 114bit（2 个 57bit 的加密比特）有效信息，其余比特有别的用处。如图 3.13 所示。

尾比特 3bit	加密比特 57bit	Flag 1bit	训练序列 26bit	Flag 1bit	加密比特 57bit	尾比特 3bit	保护间隔 8.25bit

图 3.13　普通突发脉冲序列

（2）SCH 信道的编码

SCH 信道的脉冲方式就与 TCH 有所不同。它的训练序列长达 64 位，而普通的突发脉冲只有 26 位。每个 SCH 信道有 25bit 的消息字段，其中 19bit 是帧号，6bit 用于 BSIC 号。由于 SCH 共有两个 39bit 的突发脉冲消息位共 78bit 信息。因此，我们要把这 25bit 信息编码成 78bit。

我们将这 25bit 的数据再加上 10 个奇偶校验位和 4bit 的尾位，这就得到了 39bit。再将这 39bit 按照 1∶2 的速率卷积，便得到了 78bit 的消息，如图 3.14 所示。

尾比特 3bit	加密比特 39bit	同步序列 64bit	加密比特 39bit	尾比特 3bit	保护间隔 8.25bit

图 3.14　同步突发脉冲序列

（3）RACH 信道的编码

RACH（随机接入信道）的消息是由 8 个消息比特组成的，包括 3bit 的建立原因和 5bit 的随机鉴别符。由于 RACH 的突发脉冲的消息位的字段是 36bit。因而我们需要将这 8bit 的数据编码成 36bit。

首先，我们给它加上 6bit 的色码，这 6bit 的色码是通过将 6bit 的 BSIC 和 6bit 的奇偶校验码取模二而获得的。然后再加上 4bit 的尾位。这样就得到了 18bit，我们再将这 18bit 按照 1∶2 的卷积编码速率，最后得到 RACH 突发脉冲上的 36bit 消息位，如图 3.15 所示。

尾比特 3bit	同步序列 41bit	加密比特 36bit	尾比特 3bit	保护间隔 68.25bit

图 3.15　随机接入突发脉冲序列

3.2.2　也论当校长的艺术——分集技术之交织

我们在第 2 章中讲过，由于多径效应引起的快衰落和由于障碍物引起的阴影效应对于无线通信而言都是巨大的挑战。对于 GSM 而言，这可能导致成串的突发脉冲序列丢



失；对于信道编码而言，恢复大量丢失的连续信息就显得有点力不从心。于是，我们不得不寻找更多的方式来保障空中接口的可靠性，比如下文所说的交织。

Lee 先生是 GSM 协议制定小组成员，他从麻省找了 Lucy 博士设计了 GSM 的语音编码，也就是信源编码。然后又找了 LILEI 博士来设计 GSM 的信道编码，没想到过了几天 LILEI 博士气呼呼地找了过来。

LILEI：“Lee 先生，你这无线信道是什么破信道，我搞来搞去搞不定了！”

Lee 一脸吃惊：“LILEI 先生，怎么了，还有你搞不定的？”

“是啊，这无线通信的信道状况实在是太糟糕了！”LILEI 听到 Lee 的称赞，稍微平和了一点“我按你的要求做的嘛，采样后经过信源编码、信道编码，每 20ms 的语音产生了 456 个比特。但是你这个变态的无线信道衰落这么厉害，经常产生成串的比特误差，我的信道编码可恢复不了这么多误差，我可玩不下去了！”

“你设计的一个 TDMA 帧有 8 个时隙，每个时隙可以放 1 个冲突（见图 3.16），对不对？”

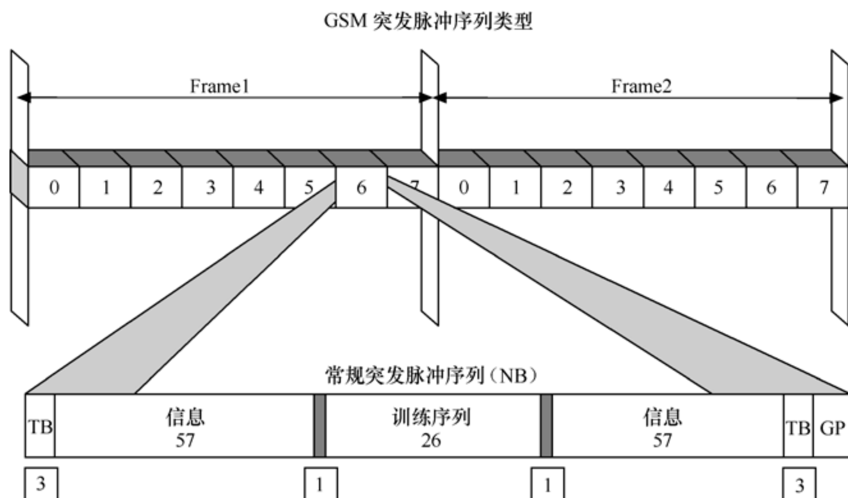


图 3.16　GSM 突发脉冲序列

“为了迎合你的设计，我把编码后的 456bit 分为 8 组，每组 57bit（如图 3.17 所示），然后把每两块插入 1 个冲突。4 个冲突就可以传完一个 20ms 的语音块。这样设计很完美了吧？然而人算不如天算啊，你这无线信道太差了，动不动就一个突发脉冲被噪声湮没掉了。也就是两个块没了，我总共就 8 个块，这还怎么玩！”

Lee 先生看完之后会心一笑：“LILEI 博士，我知道你是个很好的学者，但估计很难成为一个很好的校长。你这种排列法让我想起我中学时的校长，我现在都有点恨他，他排课表简直和你排这些比特有得一拼。你看看他这课表（见图 3.18），每次我周日玩得

57	114	171	228	285	342	399	456
56	113	170	227	284	341	398	455
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
2	59	116	173	230	287	344	401
1	58	115	172	229	286	343	400

图 3.17　LILEI 博士最初的排列设想

很疯，然后周一精神状态就很差。所以周一的地理课一下就六节课没上好，LILEI 你这种好学生应该知道，一节两节课没上好是很容易补上来的，六节课没上就完蛋了。所以我中学的地理成绩哦，555555。”

周一	周二	周三	周四	周五	周六
地理	数学	语文	英语	物理	化学
地理	数学	语文	英语	物理	化学
地理	数学	语文	英语	物理	化学
地理	数学	语文	英语	物理	化学
地理	数学	语文	英语	物理	化学
地理	数学	语文	英语	物理	化学

图 3.18　Lee 先生的第一任校长的排课表

“后来换了一个校长，他发现了这个课表存在问题，因此课表就换成了下面这样（见图 3.19）。周一每节课之间关联性很弱的，周一哪怕我请假也可以通过周二至周六的课程补回来，我的成绩一下就上来了。”Lee 继续说道。

周一	周二	周三	周四	周五	周六
化学	化学	化学	化学	化学	化学
物理	物理	物理	物理	物理	物理
英语	英语	英语	英语	英语	英语
语文	语文	语文	语文	语文	语文
数学	数学	数学	数学	数学	数学
地理	地理	地理	地理	地理	地理

图 3.19　Lee 先生的第二任校长的排课表



“所以啊，聪明的 LILEI 先生，你何不把你那些比特的排列换一种方式插进冲突脉冲里去呢（如图 3.20 所示）。这样的话，哪怕第一个冲突丢失（假设该冲突只放了下图中有灰底的块），对于 1～57 号信息，你也不过是丢了 1、9、17、25、33、41、49、57 这 8 个比特，用你的信道编码完全恢复得了。不像第一种编法，整个 1～57 号信息都丢了，哭爷爷叫奶奶都没用了。”Lee 笑着说道，随即诗兴大发，“爱交织着恨，情交织着仇。情绪事物混在一起称为交织，我们就把这个技术叫做交织吧。”

449	450	451	452	453	454	455	456
441	442	443	444	445	446	447	448
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
9	10	11	12	13	14	15	16
1	2	3	4	5	6	7	8

图 3.20　LILEI 博士最终排列

“恩，很好听的名字。在你的基础上我又在想啊，你刚刚是在 20ms 的语音块内交织。那这个 20ms 语音块和那个 20ms 的语音块之间是不是也可以交织呢？你看那 NB 突发脉冲图，它不是有两个放比特块的位置么，我没必要把这两个块都放来自同一个 20ms 语音块的信息啊，我可以放来自其他语音块的信息啊。这样，万一一个冲突两个信息块丢掉，我们丢失的这个 20ms 语音块的东西就更少了，请看下图（见图 3.21）。刚才那个叫块内交织，我这个就叫块间交织吧。”

提示：概括地说，交织就是把码字的 b 个比特分散到 n 个帧中，以改变比特间的邻近关系，因此 n 值越大，传输特性越好，但传输时延也越大，从图 3.21 中可以很清楚地看出这一点。所以在实际使用中必须作折中考虑。

总结：所谓交织技术，是为了应对无线变参信道而设计的一种干扰平均化的手段。为了克服某一条无线路径的衰落带来的失真，采用接收多条无线信道的方法，使得空间路径带来的干扰平均化，称之为空间分集；为了克服某个频率的干扰带来的失真，采用跳频的方式来使得干扰在几个载频之间平均，称之为频率分集；上述的交织就是时间分集。3 种分集技术其本质都是一样的，即通过技术手段使得在空间、时间、频率上的干扰变得平均化来克服无线变参信道的影响。

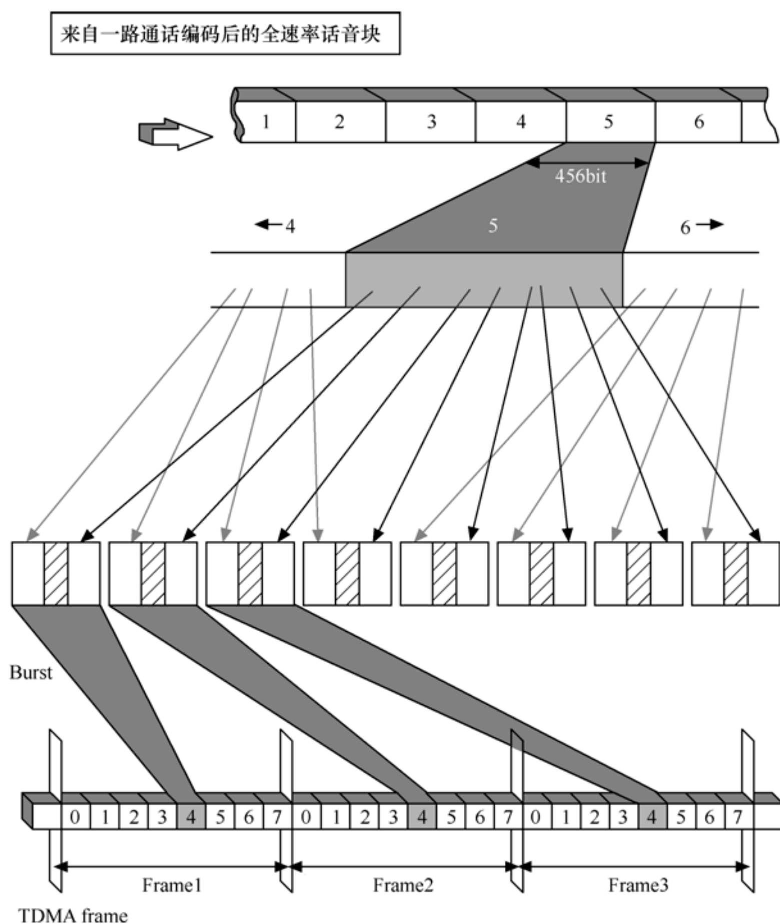


图 3.21 块间交织技术

3.2.3 当心和自家的鱼雷亲密接触哦——分集技术之跳频

我们在第 2 章讲过，除了快衰落和慢衰落，干扰也是无线通信中很头疼的一个问题。在 GSM 系统中，干扰可能来自系统内部，比如说一个用户占用无线信道发射信号时对其他用户的干扰；干扰也可能来自系统外部，比如高频噪声、汽车点火装置，甚至是信号屏蔽干扰器。当某个频点受到干扰时，我们希望换到另一个频点上，以避开干扰。实际上，跳频技术最早用于军事上，GSM 不过是借鉴而已。

无线电通信由于它的灵活和方便的特性，常常被用于战时通信。但是，传统的无线电通信都是在某个固定频率下工作的，很容易被敌方截获或施加电子干扰，使这种通信方式不再起作用。



二战的时候，盟军非常担心轴心国利用无线电信号干扰自己的无线电系统，从而导致从潜水艇发射的鱼雷偏离既定的目标，万一撞上自己人，那就很不好玩了，连个说理的地方都没有。

为此，有两个专家对此进行了研究并申请了专利。这两位专家和发明电话的贝尔先生及发明电报的莫尔斯先生一样，本职工作也与通信毫不相关，一位是管弦乐作曲家乔治 • 安泰尔，另一位是电影明星兼无线通信工程师海蒂 • 拉玛，他们利用一个中央的“权力中心”与两个终端设备进行通信，指导这两个设备随机地从一个频率跳转到另外一个频率，而且时间点和时间间隔也是随机的（比如5s），只有基地和两个设备知道什么时候跳变、跳变到哪里以及跳变持续多长时间。从外部看，这个跳频的过程似乎是完全随机地，基地精确地知道它在做什么以及什么时间做，所以跳频行为实际上不是真正的随机，因此有了个术语叫做“伪随机”。音乐家发明这种技术并不太令人吃惊，在器乐演奏上，指挥家和演奏家也有一个共同的“伪随机序列”——五线谱，这使得他们可以以同一个节拍来完成一场完美的演奏。

与盟军的无线通信系统一样，GSM 也必须考虑干扰和噪声问题，只不过这种干扰一般并非来自敌对方。GSM 也借鉴了跳频技术，不过与盟军采用的方式不同的是，GSM 跳频的时间间隔是固定的，在 GSM 规范中有严格的定义。GSM 跳频示意图如图 3.22 所示。

	TDMA 帧 1								TDMA 帧 2								TDMA 帧 3							
	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
0 号频点		■																						
1 号频点										■														
2 号频点																		■						
3 号频点																								
4 号频点																								
5 号频点																								

图 3.22　GSM 跳频示意图

GSM 的跳频分为基带跳频和射频跳频两种，什么叫基带信号，没有经过调制的信号就叫基带信号；什么叫频带，经过了调制的信号就叫频带信号。所谓基带跳频与射频跳频，其本质都是一样的，都是把 1s 的信号分成 217 份，每一份都通过不断变化的频率上发送出去，这就是所谓的跳频。基带跳频和射频跳频其不同之处在于，基带跳频“跳”的是基带信号，而射频跳频“跳”的是经过了调制的射频信号。

基带跳频如图 3.23 所示，图中可以清晰地看到基带信号在调制之前就完成了时隙交换，送到了各块载频，实现了每时隙发射频率的不断变化。

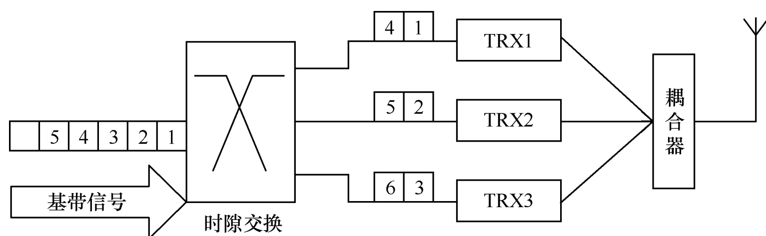


图 3.23　基带跳频示意图

射频跳频比基带跳频从理解的角度而言要略为复杂一些，因为 BCCH 载频是不能参与跳频的。BCCH 载频用于向移动台广播信息，如果 BCCH 载频的频率随意变化，那么移动台就无法锁定某个频道来接收系统信息了。如果是这样的话，那么 FCCH 频率校正脉冲和 SCH 同步脉冲也就失去了意义。图 3.24 所示为射频跳频示意图。

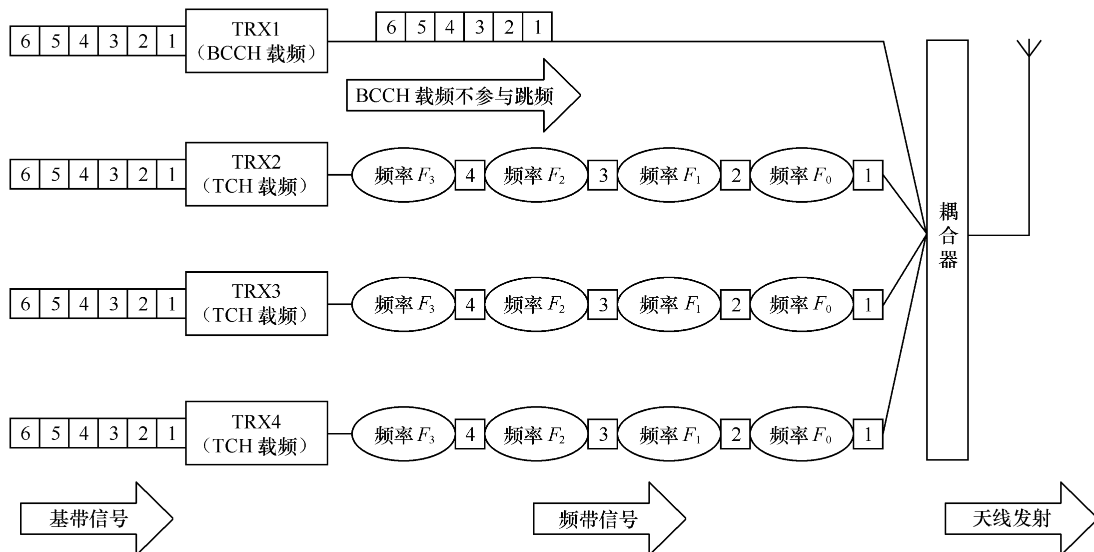


图 3.24　射频跳频示意图

以图 3.24 为例，TRX2 载频在接收基带信号之后，每个 TDMA 帧时间变换一次频率，将信号以不同的频率送到耦合器，再通过天线发射出去。

说到这里，我们不禁要问，GSM 系统中如此费尽心机地设计了跳频，到底有什么好处，它能给我们的网络带来什么？

首先，跳频可以起到干扰源分集的作用。盟军怕无线通信受到干扰而采取了不断变化频率的方法来避开干扰。GSM 同样也是如此，在业务量密集的地方，网络的容量将受到由于频率复用产生的干扰的限制。载波干扰比之值 C/I 可能在呼叫期间变化很大。如



果不选用跳频，一旦某一频点出现干扰（GSM 系统产生的同频干扰或者外系统干扰源产生的干扰），占用该频点的用户的通话质量就会差得难以忍受。如果采用跳频，该频点的干扰就会为其他呼叫用户所共享，噪声就平均化了，整个网络的性能将得到提高。频点就好比房间，如果有一个房间紧靠厕所臭气熏天（强干扰），那固定某个人住肯定是不合适的，那就只好大家轮流住了，这要大家轮流分担了痛苦，痛苦就平均化了，不至于某一个人固定在那里被熏晕（掉话）。

其次，跳频可以起到频率分集的作用。我们知道，无线信道很要命的一大杀手就是瑞利衰落。啥叫瑞利衰落？请参见 2.8 节。不同频率信号其衰落特性不同，对于相距足够远的频率，他们可看做是完全独立。通过跳频，可使携带同一部分信息的所有脉冲不会被瑞利衰落以同一种方式破坏掉。这就跟我们第 2 章里讲到的姜子牙的阴书有点相似，我的信息是通过不同的频率发送出去的，就相当于不同的道路发送出去的；只要相距足够远的频率，也就是说这些道路得有点距离，要是像 100m 跑那样一条道紧挨着另一条，那也没啥用处，横次里杀出一条野牛能把你几条道上的人都掀翻。在 GSM 里面，带宽相距大于 400kHz 就足够了，当然，更宽效果会好些。

下面我们来介绍 GSM 系统跳频里所采用的参数。终端跳频的频点用 MA 描述，MA 是基站小区配置频点 CA 的子集，MA 可以包含 N 个频点（$1 \leqslant N \leqslant 64$）。

终端的跳频方法由跳频算法所决定，可以用两个主要参数来进行描述：跳频序列号 HSN 和移动分配指数偏置 MAIO。HSN 的取值为 0～63，MAIO 的取值为 0～$N-1$，你也可以理解为 MAIO 是 HSN 的真子集，不过就一位数而已。因此，跳频算法允许有 64 种不同的跳频序列，HSN 的取值决定了具体的跳频序列，MAIO 相当于跳频序列的起始位置。

跳频序列有两种，即循环跳频和伪随机序列跳频，我们前面讲到的盟军的跳频方式就是采取的伪随机序列跳频。HSN=0 为循环跳频；当 HSN≠0 时，为伪随机序列跳频，可以根据一个伪随机序列表求出相应的跳频序列。这个有点相当于 NCC（网络色码）与训练序列的关系，NCC 的 8 种取值也对应了 8 种不同的训练序列。

通常在一个小区内不同的终端使用同样的 HSN 和不同的 MAIO，这样可以避免小区内不同的终端之间的信道干扰。相邻小区之间不会有干扰，因为它们使用不同的频率组，即不同的 MA。使用同样频率组的其他小区应该和本跳频小区采取不同的 HSN。

另外，如前所述，GSM 系统中的 C0 是不参与跳频的，相当于 N=1，MAIO=0 的情况。

注意： 跳频只是 GSM 应对瑞利衰落的一种途径，GSM 还通过信道编码（增加信号的冗余度）、交织技术（时间分集）来对抗瑞利衰落。瑞利衰落是无线通信最致命的敌人之一，我们不得不绞尽脑汁来应对这个敌人。



3.2.4 刺刀在前，刺刀在后——时间提前量（TA 值）

相信大家都看过阅兵式，也相信大家也为仪仗队整齐划一的军容军姿表示过赞叹。仪仗队的军人踢着正步，步点在时间和方位上极其精准，整个方阵看起来就如同一个人一样。请注意了，仪仗队的战士都斜刺里握着钢枪，那在阳光下锃亮雪白的刺刀离前一个人的颈窝不到 10cm，当然他后面战士的刺刀离他的颈窝也不到 10cm。可以想象，这个方阵对时间的精准性要求达到了多么苛刻的程度。你稍微踏快了点，会伤到前面的战士。你稍微踏慢点，则会被后面的人伤到。你必须每一个步点都精确地踏在属于你的空间和你的时间里。

其实 GSM 系统又何尝不是如此，由于 GSM 系统的空中接口采取了时分复用的技术，那么精准地控制手机的发射时间就变得异常重要。一个手机必须在指配给它的时间里发射信号，而在其余时间又必须保持寂静，否则它会干扰使用同样载频上不同时隙的另一些移动用户。这就如同阅兵一样，走快了和走慢了都不行，前后都是刺刀呢，会干扰到前后的人。

如图 3.25 所示的手机，它必须在它所在的第 4 号时隙发射信号，否则就会干扰旁边时隙的手机。

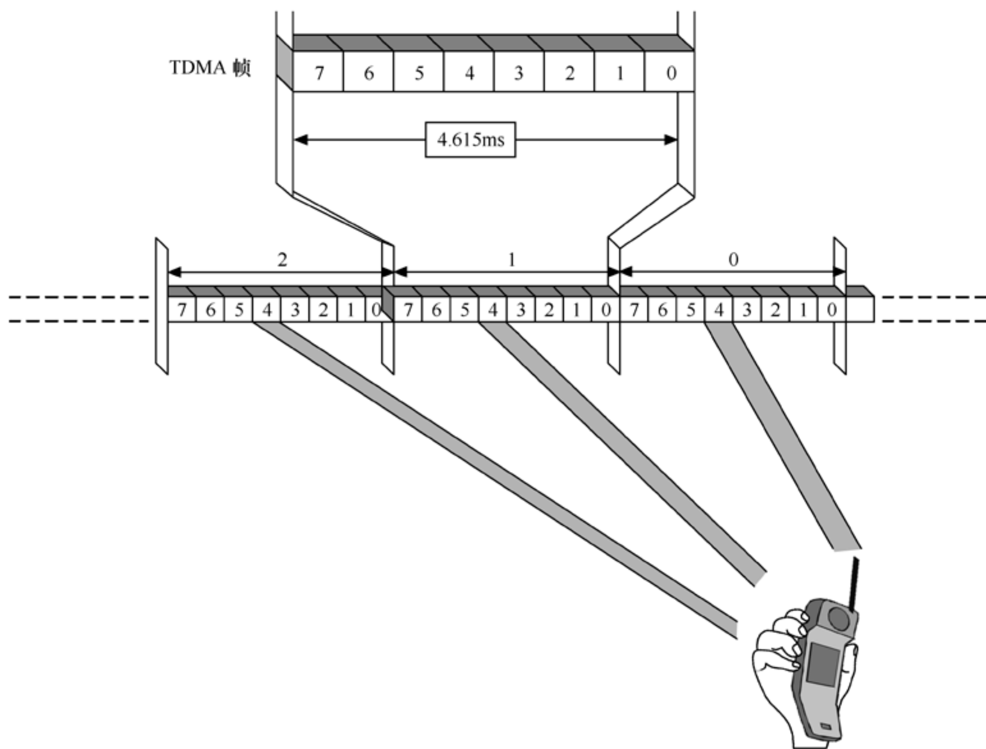


图 3.25　手机占用 4 号时隙通话



但由于手机在微观上看不是全双工模式，只有一套收发装备，所以在特定的时隙只能收或发（基站有多套收发设备），为了避免手机这个问题，规范规定上行和下行有 3 个时隙的偏移量，这样就形成了图 3.26。



图 3.26　上下行 3 个时隙的偏移

当然 GSM 系统在设计的时候不要这 3 个时隙的时间差也是完全可以做得到的，只要给手机添加一个双工器，让手机可以同时发射和接收信号即可。综合考量起来，GSM 系统的设计者还是觉得增加这么多成本不划算，于是还是把上下行设计了 3 个时隙的偏差，从而可以节省双工器的开支。

思考： 请看图 3.25，该手机在离基站基本 0 距离的时候用的是第 4 号时隙，那么该手机到离基站几千米、十几千米的时候继续使用 4 号时隙会不会有问题？电磁波在空中的传播是需要时间的，这个延时会不会导致该手机用到第 5 号时隙，从而对占用 5 号时隙的手机产生干扰？

空口无凭，我们来算算看！

我们后面会讲到，GSM 中一个比特占用的时间约为 3.7μs。

计算过程： TDMA 帧占用的时间是 4.615ms，那么一个时隙占用的时间就为 4.615ms/8 ≈ 0.577ms。一个时隙的突发脉冲有 156.25bit，那么每个比特占用的时间就约为 0.577ms/156.25 ≈ 3.7μs。

假设手机离基站 9km，那么基站至手机有一次延时，手机至基站又有一次延时，那么一来一回就是 18km。

单程延时 t_1=9 000m/(3×10^8m/s)=30μs，双程延时 60μs。

那么实际情况就变成了图 3.27 所示的情况。

60μs 可以造成多大影响呢？60μs /(3.7μs/bit)=17bit，足以造成 17bit 的延时。GSM 为了消除路径的时延，就引入了一个时间提前量 TA（Time Advance）值，指示手机提前发射，刚刚例子中所述的 TA 值就为 $2t_1$=60μs，也可以理解为 17bit。

实际上，GSM 中的时间提前量 TA 就是以比特来计算的，其取值范围为 0～63bit，对应时间为 0～233μs，对应覆盖半径为 0～35km。

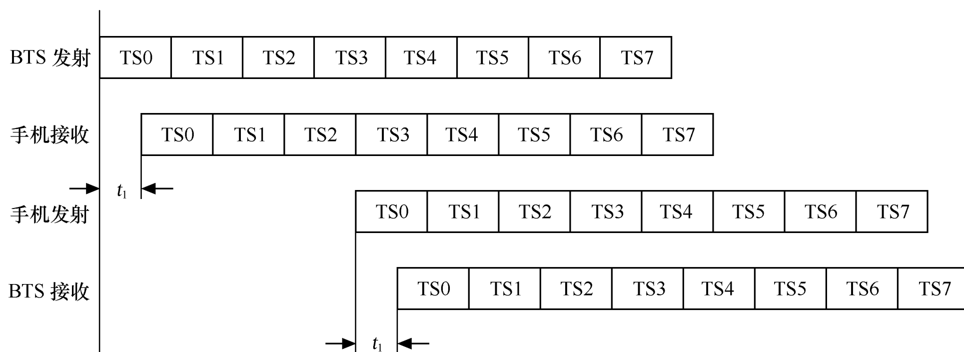


图 3.27　时间延迟

在呼叫过程中，手机必须不断测量时延值然后通过 SACCH 信道传送给基站，然后基站必须监测呼叫达到的时间，并在下行的 SACCH 的系统消息上每 0.5s 向移动台发出一次指令，逐步指示移动台应提前发射的时间。

大家或许又要问，0.5s 才指示一次时间提前量，假如我坐在动车组上，会不会因为速度太快而造成对其他时隙的干扰？我们很容易根据上面的内容换算出，要延迟 1bit，需要你移动 554m 的距离，你在 0.5s 内能移动 554m 的距离么？呵呵，除非你坐的是波音 747。最高速度 431km/h 的磁悬浮最快速度也只有 119m/s 啊。

还有一个潜在的隐患不知道大家想到没有，无线信道是有多径效应的，TA 值的测算是可能存在误差的，经过实地测算，最多可能达到 3bit 的误差。GSM 的设计者是怎样解决这个问题的呢？请看图 3.28。

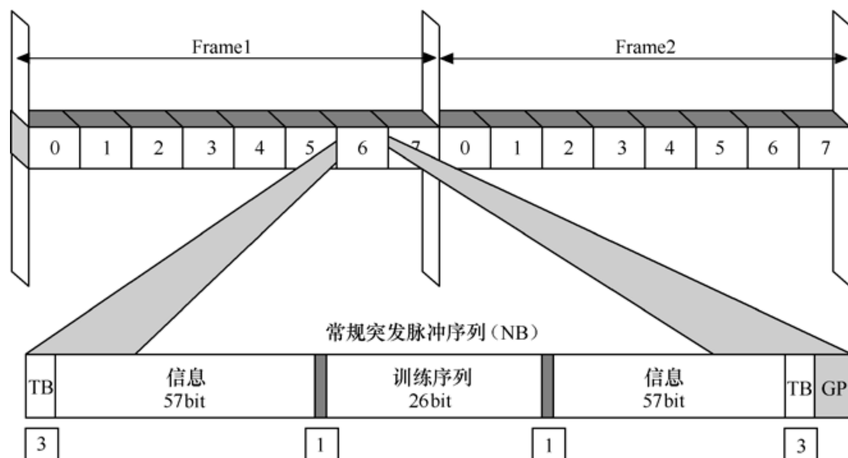


图 3.28　突发脉冲序列



设计的时候为每个突发脉冲留了 GP，也就是保护间隔。保护间隔有点类似阅兵式上为刺刀留得那 10cm，虽说方阵系统对时间的要求极其严格，但万一有点差错的时候，总得有个缓冲啊。这个保护间隔有多长？以后在讲突发脉冲的时候会涉及，在这里就不再赘述。

思考：在这里给大家出一个思考题，TA 值为什么要在 SACCH 信道里发送？SACCH 信道里除了 TA 值还发送哪些内容？为什么这些内容要在 SACCH 信道里发送？相信大家看完全书会有自己的答案。

3.2.5　训练序列的由来——时间色散与均衡

我们在第 2 章中提过，无线通信与有线通信一个重要的区别就是无线通信是采用电磁波进行传输的，其传播路径不固定。除了视距传播（又称 LOS 传播，Line of Sight）以外，它还可能产生反射、绕射和散射，由此，就产生了多条路径的信号传播。多径传播不仅带来了要命的瑞利衰落，也带来了让人讨厌的时间色散。那么什么是时间色散，我们又如何来应对它呢？

在带宽受限（GSM 每频点 200kHz 带宽，显然是带限信号）的信道中，由于多径效应而导致的符号间干扰会（即时间色散）使被传输的信号产生失真，从而在接收机中产生误码。符号间干扰被认为是在无线信道中传输高速率数据时的主要障碍。

码间干扰主要来自反射，但与多径衰落不同的是，其发射信号通常来自远离接收天线几千米远处的物体。其缘由不难理解，多径衰落是延迟半波长的时延，900MHz 的电磁波，其波长为 30cm，那么半波长就是 15cm，相隔不远。而码间干扰（时间色散）是延迟几个比特位的时间，我们在 3.2.4 节中已经讲过，延迟 1 个比特位，大概就是电磁波在空中传送 554m 的距离，那么延迟几个比特位的距离是多远，大家也很容易推算出来。

我们画一个图来帮助大家理解，由基站发送“1”、“0”序列，如果反射信号的到达时间刚好滞后直射信号一个比特的时间，那么接收机将在直射信号中检测出“0”的同时，还从反射信号中检测出“1”，于是导致符号“1”对符号“0”的干扰。由于多径传播和时延导致的误码如图 3.29 所示。

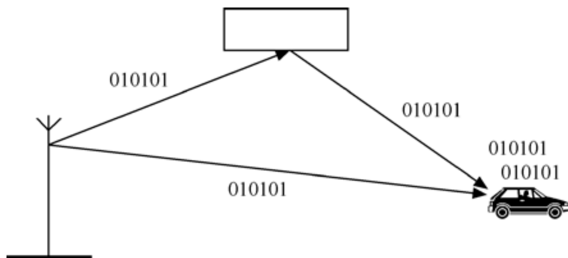


图 3.29　由于多径传播和时延导致的误码

那怎么来应对这个时间色散呢，GSM 采用的是均衡的方法。如果你对 GSM 的突发脉冲组成方式熟悉，那么你一定知道，除了 SCH 和 FCCH 这两个比较特殊一点的脉冲，其他突发脉冲如 TCH、SACCH、FACCH 等的脉冲里面都是有一个叫训练序列的 26bit 的东西。同步突发脉冲有一个长达 64bit 的同步信息，其实也可以理解为训练序列。（如果对 GSM 突发脉冲不熟悉，那没关系，我们会在后面介绍空中接口的物理层时讲到。）

我们知道，空中接口的资源是很宝贵的，一个 TCH 脉冲，总共 148bit，有效的语音信息只有 57×2=114bit，而一个训练序列就有 26bit，它的开销比用于定位的尾比特以及用于防止时隙间相互干扰的保护间隔的总和还要多。它到底是谁？它是做什么的？它为什么要消耗这么多资源？一串串问号不由得在我们脑海里浮现。

训练序列在 GSM 里面的作用其实就是树立一种标准，这种标准用于帮助基站来衡量和判断无线信道的情况并在接收信号的时候予以校正，保证最佳的接收效果。值得注意的是，无论是发射端还是接收端，事先都是知道训练序列的。发射端比如手机，把这个 26bit 的训练序列通过空中接口发送出去，基站接收到信号以后，把训练序列从第一个比特到最后一个比特和自身的核对一遍，发现完全一致。那么很好，这个无线信道太完美了，什么都不需要做，对于 TCH 的语音信号，照单全收就是了。通常情况下事情不会这么顺利，如果发现有些比特位的信息是错的，和约定的不一致，那么就需要对滤波器的一些参数进行调整，以保证最好的接收效果，这个滤波器就是均衡器。

GSM 里确立了 8 种训练序列，每个小区在定义了 BSIC 的时候就定义了该小区载频所采用的训练序列。为什么？因为 BSIC=NCC（3bit）+BCC（3bit）。大家注意这个 BCC 有什么特点？除了 3bit 的位长似乎没有别的特点，那么 3bit 可以表示多少信息，我们由二进制很容易得到 $2^3=8$。呵呵，正好是可以表示 8 种不同的信息，实际上，在 GSM 里面，就是用 BCC 来定义某个小区所采用的训练序列。

上面我们说了，小区里所有载频所采用的训练序列是通过 BSIC 定义的，早就在网络管理系统上定义好了。那么手机怎么知道它所在的小区采用的是哪个训练序列，并与其保持一致呢？

这就需要小区来告诉手机了，小区会在它的 BCCH 广播信道上下发 SCH 同步消息，而 SCH 同步信息就包含了 BSIC 号。手机对 SCH 信道解码以后，自然就知道了训练序列，如图 3.30 所示。说到这里，我想大家也一定明白了 FCCH 频率校正突发脉冲和 SCH 同步突发脉冲为什么没有训练序列了，还没有锁定以及同步好一个小区，根本就不知道 BSIC 号，也就无从谈起什么训练序列了。

我们也许还要问，为什么每个 TCH 突发脉冲都要带一个训练序列，这样多消耗资源啊，能不能就第一个 TCH 突发脉冲带一个训练序列让接收器测算一下无线信道的特性，



NCC	训练序列																								
0	0	0	1	0	0	1	0	1	1	1	0	0	0	0	1	0	0	0	1	0	0	1	0	1	1	1
1	0	0	1	0	1	1	0	1	1	1	0	1	1	1	1	0	0	0	1	0	1	1	0	1	1	1
2	0	1	0	0	0	0	1	1	1	0	1	1	1	0	1	0	0	1	0	0	0	0	1	1	1	0
3	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0
4	0	0	0	1	1	0	1	0	1	1	1	0	0	1	0	0	0	0	0	1	1	0	1	0	1	1
5	0	1	0	0	1	1	1	0	1	0	1	1	0	0	0	0	0	1	0	0	1	1	1	0	1	0
6	1	0	1	0	0	1	1	1	1	1	0	1	1	0	0	0	1	0	1	0	0	1	1	1	1	1
7	1	1	1	0	1	1	1	1	0	0	0	1	0	0	1	0	1	1	1	0	1	1	1	1	0	0

图 3.30　训练序列

以后的就不要再带了，免得浪费？这个想法很好，但是忽略了无线信道一个特点，即时变。无线信道的特性无时无刻不在变化，这 20ms 无线信道的特性不能代表下 20ms 无线信道的特性，所以每个 TCH 突发脉冲都不得不携带一个长达 26bit 的训练序列以保证最佳的接收效果。这个开销的确很大，但是对于无线信道这么一个差错奇高、性能奇差的信道而言，这些开销是合理的。一路上到处是绿林好汉劫径，你说你能不多带几个保镖么？

说到这里，我们依然没有回答两个问题，一是用于解决时间色散问题的这个自适应均衡器到底是怎样工作的，二是为什么 GSM 的训练序列要有 26bit 这么多？这是一个非常复杂的数学问题，为了本书的读者不至于看得头晕目眩，作者不打算在这里对这个问题加以铺开阐述，有兴趣的读者，可以翻看参考文献 6 的第 7 章，那里对均衡原理及其实现有很详尽的阐述。

注意： 在本节中大量提到了本节之前完全没有涉及的一些知识，比如 FCCH、SCH、BSIC，这都是属于 GSM 空中接口物理层的知识，我们会在后面的章节中对这些内容进行详细讲解。本书有些章节之间的内容是有交叉的，后面的内容在前面可能会涉及，前面的内容在后面也可能要进行重复介绍，知识点之间很难完全割裂开来，希望读者对此予以注意。

3.3 如何降低手机的功耗及对系统的干扰

我们在 3.1.3“空分复用”这一节里已经提到了这样的观念，很多 GSM 手机额定功

率只有区区 2W。把手机的额定功率做得更大并不复杂，只要你不怕把手机做得像砖头一样就行。问题是把功率做大与 GSM 设计之初的理念恰好相悖，GSM 所希望的并不是通过提高发射功率来扩大使用范围，而是在可以接受的范围内尽量降低发射功率来进行频率的空分复用。

GSM 是这样理解无线通信的：GSM 认为空中接口的频率是最稀缺的资源，因此频率一定要多加利用，反复利用！具体的措施就是小区分裂，通过控制基站和手机的发射功率，从而降低对邻区以及更远区域的电磁干扰，尽量提高频率的复用程度。在这个环节里，GSM 系统采取了每 480ms 调整一次手机发射功率的方式来降低手机对系统的干扰。

另外，据统计结果，通话时某一方只有 40%的时间是在说话的，那么 GSM 手机采用了一个 VAD（Voice Active Detect，话音激活检测）技术来测量你是否在说话，如果在说话，那么向对方传送 13kbit/s 的语音信号；如果不在说话，那么就只向对方传送 0.5kbit/s 的舒适背景噪声。这项技术称为 DTX（Discontinuous Transimission，不连续发射）相对而言也降低了 GSM 系统总体的干扰。

再者，GSM 是一个商业系统，一个商业系统最重要的一点就是要把客户需求放在第一位。客户都希望自己的手机小巧、漂亮、方便携带、待机时间也要长。要满足客户的需求，一方面有赖于工艺水平的进步，另一方面就是标准的设计也必须进行考虑。GSM 系统中，采用了 DRX（Discontinuous Reception）技术，即把手机分成不同的寻呼组，当没有轮到属于自己的寻呼组时，该手机可以关闭一些器件，进行休眠，以降低耗电量。

3.3.1 请小点声，再小点声——功率控制

对于目前的这些无线通信方式，功率控制都是一个很重要的命题。因为空中接口的频率资源有限，有限就必须要复用，复用就必定会产生系统内部的干扰，有干扰就必定要求我们的发射功率可以在可接受的范围内小一点，再小一点，以尽量降低干扰。

注意： 我们已经很多次提到了空中接口频率资源的稀缺性了。在这里，我想再啰唆一句，虽然功率控制对克服大尺度衰落和小尺度衰落不无帮助，但其产生的最根本的原因还是这种稀缺性，如果不是因为这种稀缺性导致需要进行复用（频分复用、时分复用、码分复用），我们原本不需要把功率调来调去、调大调小，按最大功率发射就是了。就比如你那台只收不发，不需要任何复用技术的收音机来说，它可需要进行什么功率控制？嘿嘿，同是玩无线技术，广电系的同学比电信系的幸福啊。



对于 GSM 和 CDMA（以及 3G）技术而言，功率控制的要求是有着很大不同的。

GSM 是频分复用，每 200kHz 划一个频段，如果某一个手机发射功率过大，干扰的也就是附近占用同频和邻频的手机，相对来说情况还不那么严重。因此 GSM 采用的是通过慢速随路控制信道（SACCH）来发送手机的发射功率，每 480ms 一次，每秒也就能修改两次发射功率，2Hz 差不多也够用了。

对于 CDMA 来说，这个要求就要苛刻得多，因为 CDMA 各个设备采用的是同一个频率（一般情况下），通过不同的码片来区分不同的终端。然而尽管 CDMA 系统中的不同设备可以用不同的扩频码来区分，但是对于解调器来说，其抗干扰特性决定了能接受的干扰信号的强度是有限的。因此，对于 CDMA 技术而言，为了防止一个用户发射功率过大从而阻塞整个小区的用户，其功率控制的频率比 GSM 要高得多，比如 IS-95，基站每 1.25ms 就向终端发一次功率调整指令，其频率约为 800Hz，而 WCDMA 的则高达 1 500Hz。

上面的说法或许不够形象，理解起来有点困难。我们可以换一种说法，GSM 好比在 KTV 唱歌，频率复用就是用一间一间的房间把用户给隔开，这样你嗓门再大顶多影响你这个房间的人说话（同包厢干扰——同频干扰），再不济顶天吵到隔壁（邻包厢干扰——邻频干扰）。

CDMA 不同了，就好比在一个会议室大家互相交流，大家随便用英语、日语或者中文交流（不同的码），说话的人虽多，也可以不被别人干扰。比如俺，就只懂中文，管它英语日语法语意大利语世界语，在俺耳中通通都只当是背景噪声，俺的解扩码是中文，俺可以准确地从一堆说话的人中分辨出中文。但是，如果有一个说世界语的嗓门特别大，就如同加了一个大喇叭一样，那咱谁也别指望能听清谁说话了。这时候会议室的主持人就会按捺不住了："说世界语的那位同学，请小点声，再小点声，这可是公共场所，咋不知道文明点呢，你要跟大家声音大小差不多咱才好交流嘛；还有那个说津巴布韦语的同学，你嗓门放大一点，你对门都快听不清你说什么了"。

呵呵，对"会议室"里说话的同学的音量的控制，自然要比"KTV"里严格得多。

对功率控制的原因和原理有了基本的了解以后，我们现在来关注更加实际的问题，那就是对于一个实用的无线通信系统比如 GSM，它的功率控制具体是怎样实现的呢？

手机在小区移动时，它的发射功率需要变化。当它离基站较近时，需要降低发射功率，以减少对其他用户的干扰；当它离基站较远时，就应该增大发射功率，以用于克服增加了的路径衰耗。

在 GSM 系统中，无论是基站还是手机的发射功率都是由 BSC 来进行控制的，而并不是基站和本身，这也是无线资源（RR，Radio Resource）管理的重要内容。发射功率的调整往往取决于两个因素，一个是接收电平，另一个是接收质量（误码率）。在这里提



一句，接收电平和接收质量几乎是衡量一条无线链路质量的标准公式，我们在潜意识里往往只考虑接收电平（手机有几格信号）而忽略了接收质量（信号的失真度），因为后者往往很难像前者一样有直观清晰的参考标准。

我们把手机的功率控制划分为进入连接模式之前和进入连接模式之后，为什么要这样划分呢？

因为手机进入连接模式之前和 BSC 根本就没有信息交换，BSC 是没法实时指导手机应该如何如何。实际上也没有这个必要，手机进入连接模式，实现和网络的连接之前跟收音机差不多，只收听 BCCH 的广播，别的基本啥事也不干，也不会对网络造成什么干扰。

但是 BSC 还是决定对空闲模式的手机进行文明礼貌教育，告诉它们第一次接入系统时最大的信道发射功率。处于空闲模式的手机，就像慵懒地躺在操场上晒太阳的学生，学校是教书育人的地方，通过 BCCH 广播一刻不停地灌输思想，比如它通过 BCCH 广播告诉晒太阳的同学们，当你想听课了（进入连接模式），你必须到教室门口喊报告（通过 RACH 接入网络），你的嗓门不能高于 70dB（BCCH 广播规定该小区手机初始接入最大发射功率），否则就会影响其他同学听课咯。当然，你在门口喊报告的时候肯定会喊到 70dB，不然声音小了，老师听不到，不放你进去，你也只得在门口站着。GSM 手机也不傻啊，它接入信道的时候也是按 BCCH 广播里规定的最大功率发射的，生怕基站听不到。

用术语概括一点地说，在初始连接的时候，手机根据在空闲模式时通过收听 BCCH 广播的系统消息所得到的手机在信道上的最大发射功率参数，来获得在该小区的最大发射功率。那么当手机通过随机接入信道 RACH 接入网络时，就以 BCCH 规定的最大发射功率来进行发射。如果手机本身的功率低于这个值（很少见），那么就以手机的最大发射功率进行发射，也就是说，如果系统说你接入这个信道时信道规定的最大发射功率可以是 2W，而手机实际最大的发射功率只有 1W，那么你就按 1W 发射吧。

一旦进入了专用模式（连接模式），手机就会不断和无线网络交换信息，那么控制手机的发射功率就会变得非常重要。基站对上行链路的接收电平和接收质量（我们上面说过这是衡量无线链路质量最重要的两个标准）进行测量并传送给 BSC。至于手机当前的发射功率，是手机通过 SACCH 慢速随路信道传送给 BTS，由 BTS 传送给 BSC。BSC 对以上因素加以考虑，并考虑手机本身的最大发射功率，然后决定如何对手机发射功率进行调整。

BSC 如果决定要调整手机的功率，那么就在下行的 SACCH 信道的第一层报头里设置改变手机功率的命令和改变时间提前量（TA）的命令。有关时间提前量的概念，我们已经在 3.2.5 节里探讨过。当手机收到专用信道上 SACCH 报头中携带的功率控制命令后，就改变自己的发射功率，按该值传输。不过手机也不是神仙啊，如果改变得太多的话，



那么还是需要一点时间的，手机的功率的最大变化速度是每 13 帧（60ms）以 2dB 的速率进行变化。上行功率控制的范围是 20～30dB，步长是 2dB。

在 GSM 系统里，不仅仅是上行功率需要进行调整，下行功率也往往需要进行调整。在 GSM 系统里，这是一个可选项，你可以设置是否对基站的载频进行功率控制。值得注意的是，基站的 BCCH 载频是不参与功率控制的，因为小区内的手机是需要检测 BCCH 载频的电平从而进行小区选择和重选的，功率的变化会让手机在选择小区上无所适从。类似的，如上节所述，BCCH 载频也不参与射频跳频的，否则手机就无法锁定它了。

在下行链路上，手机会测试下行链路的接收电平和接收质量，并形成测量报告。将测量报告通过 SACCH 传送到 BTS，最后由 BSC 决定是否要进行功率控制。

我们前面说过，功率控制其根本的目的是为了降低对系统的干扰。而且我们讲过 CDMA 技术相对 GSM 技术，功率控制要重要得多，我们不妨来看看 WCDMA 的功率控制是如何实现的。

CDMA 里面有一个很让人恼火的效应，叫做远近效应，如图 3.31 所示。

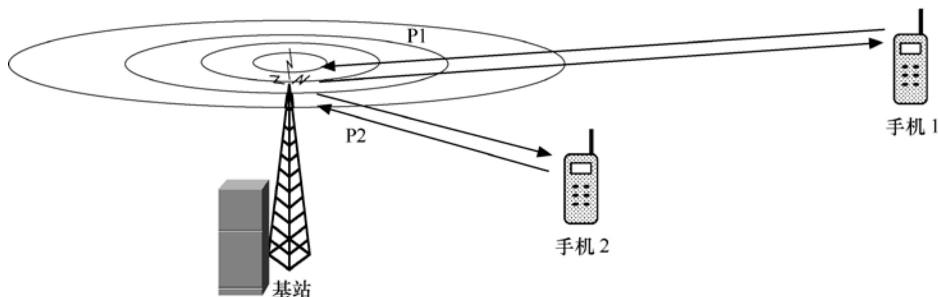


图 3.31　远近效应

移动台 1 和移动台 2 工作于同一个频率，基站只能通过它们各自的扩频码来区分它们。如果移动台 1 处于小区边缘，而移动台 2 处于靠近基站的位置。那么移动台 1 的路径损耗显然比移动台 2 要大得多，如果不对这些移动台的发射功率进行控制，那么基站收到的移动台 2 的发射功率很容易远大于移动台 1 的功率，从而阻塞移动台 1 的通信，乃至阻塞整个小区的通信。近的欺负远的，这就是 CDMA 技术中的“远近效应”。这个效应很好理解，你坐在靠近黑板的第一排，还对着老师大声说话，那么坐在最后一排的同学对老师的提问，老师就基本上听不到了。

WCDMA 所希冀的是，在任意一个时刻，基站所收到的移动台的信号，最好每一个比特的功率都相等，这样就不会有远近效应，不至于一个信号干掉另一个。那 WCDMA 的功率控制具体是怎样实现的呢？

WCDMA 在上行链路上采取的是快速闭环功率控制，说是快速，有多快？每秒

1 500Hz，不仅比大尺度衰落的速度要快，甚至比多数情况下瑞利快衰落的速度还要快。大家都知道瑞利快衰落对于无线通信是个很要命的东东，WCDMA 的功率控制技术能够对抗瑞利衰落，这实在令人很欣慰。

在上行链路的功率控制中，基站要频繁地测算接收到的信号的信干比（SIR）的值，并把它和目标 SIR 值进行比较，如果测得的 SIR 大于目标值，基站就命令移动台降低功率；如果测得的 SIR 值小于目标值，基站则命令移动台加大功率。如图 3.32 所示。

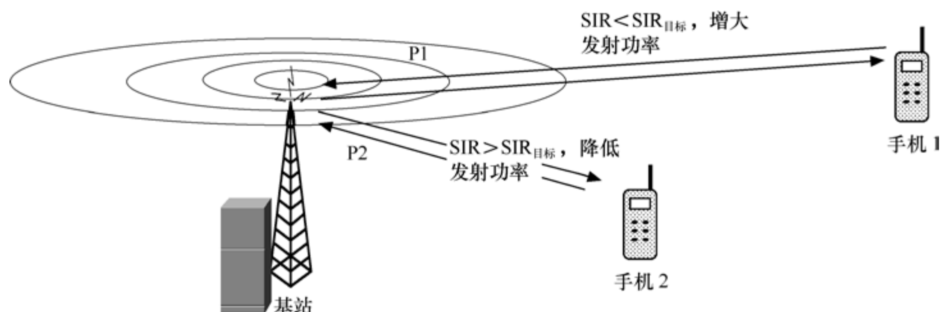


图 3.32　上行链路快速闭环功率控制

我们也可以从图 3.33 中很清楚地看到快速闭环功率控制是如何应对瑞利衰落的。

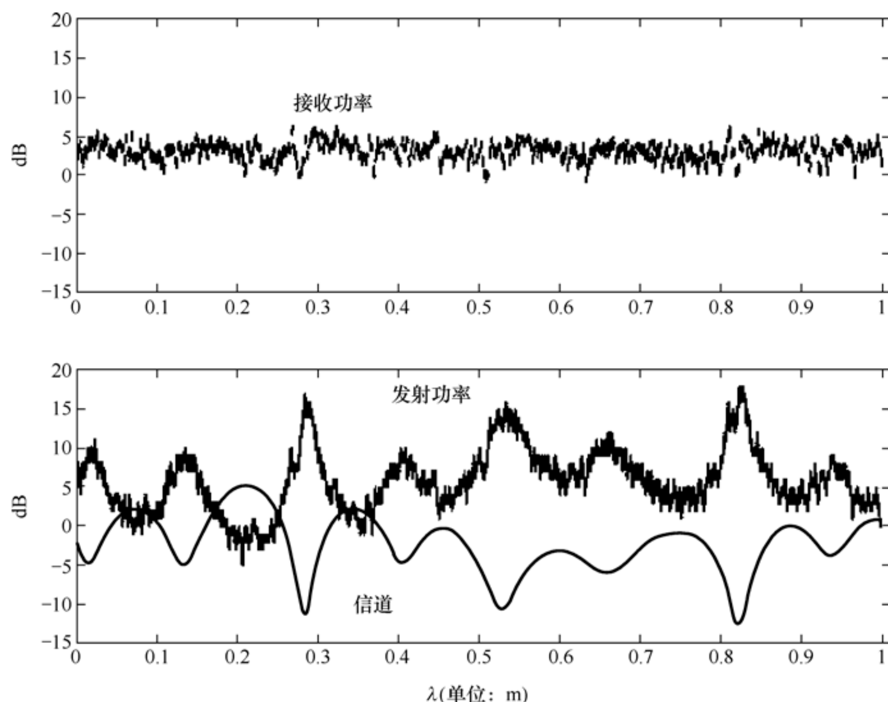


图 3.33　快速闭环功率控制对瑞利衰落的补偿



在遭遇瑞利衰落的同时，手机在基站的指示上增大发射功率，从而弥补信道上的损失，使得基站接收功率趋于平坦。

在这里，我们还要提到一个问题，即目标 SIR 值是可以变化的，为什么这个值是可以变化的呢？我们之前在提到无线链路质量的时候就提到了两个指标——电平值和接收质量（误码率），电平值只是衡量的一个标准，并不是唯一。在 WCDMA 里，调整目标 SIR 是为了追求恒定的接收质量，这个接收质量通常用误比特率（Bit Error Rate，BER）和误块率（BLER）来描述。在 SIR 恒定的情况下，移动台的速率的不同和多径的不同都会导致误码率的不同，如果要追求恒定的误码率，那么 SIR 的要求当然会有所变化。这样的考虑是自然的，假如我要得到一个 1%的误码率，在高速移动和无线环境比较恶劣情况下自然要求目标 SIR 是比较高的。如果移动速率很慢，那么原先的目标 SIR 值就显得有点浪费。

在 WCDMA 里，某个 Node B（相当于基站）的目标 SIR 值的变动是通过无线网络控制器 RNC（Radio Network Controller，相当于 BSC）来控制的，我们称之为外环功率控制。通常是这样实现的，给上行链路的每一个用户加上“帧可靠性指示符”的标签，如果帧质量指示符显示传输质量在下降，那么 RNC 就会把目标 SIR 值设高，如图 3.34 所示。

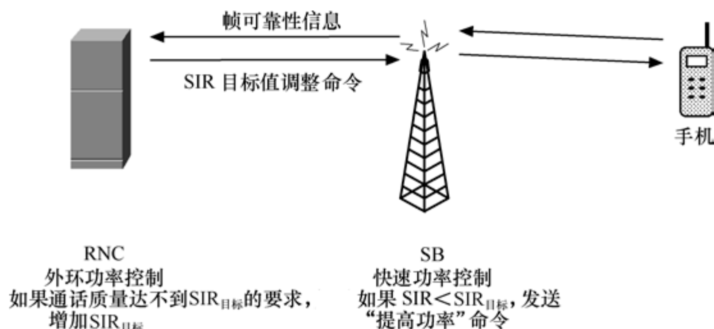


图 3.34　外环功率控制命令

3.3.2　无话可说时就请闭嘴——不连续发射（DTX）

我们都知道有一类人是很不受人待见的，那就是明明无话可说还偏偏废话连篇的人，比如说大话西游里的唐僧。这类人不招待见的原因是我们都希望有个清净的环境，不希望总被噪声干扰，因为城市里的生活已经够喧闹嘈杂了。

对于 GSM 系统来说也是如此，由于手机的通话是双向的，经统计，某个用户拿手机打电话的时候，平均的说话时间约在 40%以下。我们知道，语音经过信源编码的速率



为 13kbit/s。你说话的那 40%的时间，这个比特流量当然是不能少的；当你不说话的那 60%的时间，还以这个速率进行传输那就很令人郁闷了，因为不说话的时候传递的比特信息流对通话双方而言没有任何意义，还会对无线网络进行干扰。

如果一个人喋喋不休地在讲废话，我们通常会建议他闭嘴，别打扰别人的生活，让世界清静一点。我们自然而然地会想，我们不说话的时候，能不能就让移动台在话音信道上一个比特也别传送出去，免得让这些毫无意义的信息流对网络造成干扰。然而作为一个商业系统的 GSM，这种方案实际上并不可行，因为打电话的时候是看不到对方的，如果有一阵听不到对方的任何声音，你会怀疑对方是不是已经掉话了，这就是打电话与面对面交流的不同。面对面的时候，你让一个人闭嘴，你依然可以通过视觉知道这个人还在这里，不会认为他已经哑巴了或者人间蒸发了。

GSM 作为一个商业系统，肯定不希望为了减少手机对系统的干扰就让客户频繁产生掉话的错觉。GSM 作了一个平衡与折中，那就是在不说话的那 60%的时间，传输 500bit/s 的低速编码，这种低速编码通常被称为“舒适噪声”编码，由接收端的解码器产生舒适噪声，以避免对端的用户误以为通信已中断。

在通话的时候采取 13kbit/s 的语音编码，在通话的间隙传输 500bit/s 的低速编码，这就是 GSM 系统里减少干扰的一种方式，称之为不连续发射（Discontinuous Transimission，DTX）。

要实现不连续发射，电源就必须能够检测何时要求发射，何时只要求发射舒适噪声。在 GSM 系统里，采用的是话音激活检测（Voice Activity Detection，VAD）技术，由编码器来检测是否有声音发出。

> **注意：**BCCH 载频是不采用 DTX 技术的，道理与 BCCH 载频不参与功率控制是一样的，因为手机必须检测邻小区 BCCH 载频的电平，以便于进行小区选择和切换，采用 DTX 技术会让手机的上述过程无所适从。

采用 DTX 技术有两大好处：一是降低空中接口总的干扰电平，提高频率利用率；二是节省无线发射机电源的耗电量，延长手机电板的使用时间。

它的缺点是当上下行都采用 DTX 技术时，语音质量会受到一定程度的影响，毕竟 VAD 检测技术不一定那么精准。

通常运营商可以自行设置参数决定是否 DTX。

3.3.3 老师不点名我就继续睡觉——不连续接收（DRX）

我们都知道大学里有一类学生，称之为“特困生”。这个特困生与经济状况没什么关系，与上课的精神状态有关系。想当年，我们是四个小班组成一个大班在阶梯教室上课，“特困生”就在其中呼呼大睡，老师点名查人不到本班是绝对不肯起的，要养足精神，以



待在“传奇”或是“魔兽世界”里搏杀。

和“特困生”的精力一样，GSM 手机蓄电池的电量也是很有限的，好钢要用在刀刃上，自然不能随便浪费了。我们在上一节里提到了一种节省电量的方法——DTX，这一节里再介绍一种节省电量的方法——不连续接收（DRX，Discontinuous Reception）。

所谓的不连续接收，指的是不连续接收寻呼消息。GSM 系统通过 PCH 信道下发寻呼消息，用于寻找手机。这个寻呼消息，与寻人启事也没有什么本质的区别，都是通过广播来找手机/找人。差别当然是有的，你的家人一般是知道你在哪儿，不是非常特殊的情况是不会来个寻人启事的；而 GSM 网络并不知道你的手机具体在哪儿，所以每次与你的手机通信，都必须来个“寻机启事”，因此这个寻呼消息多得那是满天飞，即使比起牛皮癣广告和垃圾短信来也不遑多让。

对于 GSM 手机来说，面对比蝗虫还多的“寻人启事”消息自然是很令人心烦的，因为 99%以上的时间要找的并不是你，而解码 PCH 信道的消息是需要很多能量的。“特困生”也面临和 GSM 一样的麻烦，竖起耳朵听老师点名当然比趴着睡觉要消耗更多的能量，所以点名还没有到本班的时候干脆就直接忽略不劳神去听。GSM 也吸取了这种偷懒方式，GSM 按 IMSI 号把手机划分为不同的寻呼组，没有轮到寻呼自己这个组的时候，GSM 手机处于睡眠状态（也就是待机状态），对于网络的寻呼消息直接忽略；当寻呼到本组时，GSM 手机开始对 PCH 信道的消息进行解码，查看下“寻人启事”要找的究竟是不是自己。

通常解码 PCH 信道寻呼消息的时候手机的电流是几十毫安，而睡眠状态手机的电路包括 26M 晶体都不工作，耗电量通常少于 1mA，差别可不小，这就是不连续接收 DRX 的好处。图 3.35 所示为 DRX 的示意图。

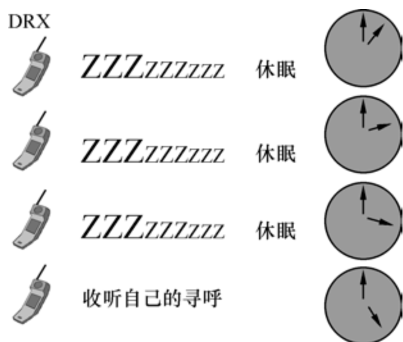


图 3.35　DRX 示意图

下面我们探讨一下怎样设置寻呼组，设置寻呼组当然希望每个寻呼组里所在的手机数量基本均匀，要不某一个寻呼组里有 1 000 部手机，另一个寻呼组才 50 部手机，网络的信令负荷就会忽大忽小，那显然不合适。俺们军训的时候，想把一个长队列分成 3 列通常就让大家报数，报数 1 的组成一列，报数 2 的组成一列，报数 3 的组成一列。GSM 也吸取了这个经验，SIM 卡不是有 IMSI 号嘛，那就按 IMSI 编号来分组。

我们上面介绍的是怎么把手机进行分组，还有一个问题就是要分几组？在 GSM 里由以下 3 个参数决定。

CCCH CONF（公共控制信道配置）：这个参数决定一个 BCCH 复帧中 CCCH 消息

块数。我们打个比方说说这个参数决定了一个电视台拿出多少时间来做公益节目——俺们这里的公益节目指的是“寻人启事”（PCH 信道）和被找的人看到寻人启事后给电视台打电话连线亲人的“亲情热线”（AGCH 信道）。

BS AG BLKS RES（接入准许保留块数）：这个参数决定了一个 BCCH 复帧中 AGCH 消息块数的数量，因为下行链路上，CCCH 信道里只有 AGCH 和 PCH 两种信道，所以这个参数实际上决定了 AGCH 和 PCH 在 CCCH 上占用的比例。就好比说 CCCH CONF 决定了一个电视台每小时拿出 9 分钟来做公益节目，然后 BS AG BLKS RES 决定拿出 3 分钟做“亲情热线”（AGCH 信道），另外 6 分钟做寻人启事（PCH 信道）。

BS PA MFRMS（寻呼信道复帧数）：这个参数实际上决定了将一个小区的寻呼信道分成多少子信道。

电视台自从开通“公益节目”后每天要接到大量的寻人启事，播音员感到有点委屈，因为她经常觉得有时候那 6 分钟播不完，有时候那 6 分钟闲得慌。台长觉得很不爽，就说她：“你不知道把资料分下组啊。这些人不都有身份证吗，我们把这些人分成 3 组。拿身份证号（IMSI 号）除以 18，能整除的一组，整除余 1 的一组，整除余 2 的一组……这样就分成 18 组了吧”。

那么这 6 分钟（一个 BCCCH 复帧中的 6 个 PCH 子信道）就这么办，第 1 分钟念第 1 组，第 2 分钟念第 2 组，第 3 分钟念第 3 组，第 4 分钟念第 4 组……好像不够 18 组啊，这样吧，下个小时和下下个小时也算进来。这样我们就有 3 个时间段了（BS PA MFRMS=3），那么我们就有 6×3=18 个时间块了。6（CCCH CONF−BS AG BLKS RES=9−3）×3(BS PA MFRMS)=18 个 PCH 寻呼子信道。

由于复帧的内容十分复杂，在学习该部分内容之前作者不打算对 CCCH CONF、BS AG BLKS RES 和 BS PA MFRMS 的用法进行详细介绍，仅做个类比供读者参考。

实战篇

“纸上得来终觉浅，绝知此事要躬行”。实验室里的通信系统是一个经过抽象的理想化的模型，而一个实际的商业无线通信系统将要面临众多问题，考虑许多因素。学习和思考一个真正的无线通信系统是如何“一砖一瓦”构建的，可以加深我们对无线通信技术的理解。

第4章 Chapter 4



商业蜂窝通信系统的典范——GSM

4.1 引言——从实验室通信走向商业通信

如果说第 2 章、第 3 章我们侧重的是无线通信理论知识的学习的话，那么从 4 章往后则偏向于介绍具体的商业无线通信系统。应当说的是，我们在之前的学习中强调的是无线通信的一些特性，并没有过多地考虑它的商业应用。

这也就是说我们之前要考虑的是如何有效地构架一个通信系统就够了，而对于蜂窝通信系统这样的商业通信系统，这些并不足够。我们除了要考虑一个通信系统的有效性外，还必须考虑它的商业属性。

所谓的商业属性，也就是两条：一是资源的分配。现代的蜂窝通信系统是个庞大的系统，一个庞大的系统必定拥有很多的资源，而所有的资源必定都是有成本的，那么如何将这些资源合理有效地分配给用户，从而达到资源利用效率的最大化，显然是个很重要的命题。比如说空中接口的频率是如此之有限，该如何进行管理，这就是 RRM（无线资源管理）的内容。同样的，Abis 接口和 A 接口的电路也同样存在资源分配问题，很多时候我都觉得，与其说这些问题是技术范畴的内容，还不如说它是管理学范畴的内容，甚至都可以从银行如何管理排队人员和窗口资源上找出其中的共性。

其二是如何满足用户需要，那些经典的通信教材，比如《通信原理》或者《无线通信原理》是不需要考虑这部分内容的，这些教材其价值在于提炼，在于抽象，在于找出各通信系统之间的共性，然后得出构架一个通信系统的一般方法，所以其内容往往在“采样—量化—编码—交织—调制—解调—去交织……”这个范畴内打转，如果超出这个范畴，那么它就要面对众多通信系统的众多实际问题，那它就不是教材，而是百科全书了。而一个实际的商业通信系统，比如 GSM、CDMA 或 PHS，就必须要考虑这个层面的问



题，因为运营这个系统的运营商每天都要面临和竞争对手之间的博弈，谁更能贴近市场的需求，谁就更容易在激烈的市场竞争中取得优势。

我们要考虑用户的漫游，所以诞生了 HLR 和 VLR。当用户办卡时，当地运营商把用户资料输入 HLR；当用户漫游到别的城市时，漫游地的 VLR 把用户资料从 HLR 复制过来，用户就可以继续享受运营商的通信服务了。

我们要考虑无线资源的有效管理，要考虑用户的无缝切换，所以收发信机的业务承载功能和控制功能就慢慢地分离了，BTS 和 BSC 各司其职，一个专门负责“采样—量化—编码—交织—调制—解调—去交织……”这些经典的无线通信工作；另一个的眼光就要更宏观一点，要着眼于资源的调度和管理以及 BTS 之间的协调。你不妨把点对点的通信看成是一个皮包公司，慢慢地做大了，做到了移动通信网这个规模，就要有业务和管理的分离，就要有业务员和部门经理，有层次才有效率。世界上很多道理其实都是相通的，这很有意思。

在计费这个层面，也越来越由技术导向转向市场导向，我们知道，如今的漫游费是被叫比主叫便宜，而且是在不断降低的，被叫资费比主叫资费低其实是一种战略层面驱动的结果。这个战略就是市场导向战略，换句通俗一点的话讲就是“用户至上，用心服务”，体现在计费层面的必然结果就是计费应当更适合用户的需求。其实从技术层面而言，以前的计费方式，即漫游时被叫比主叫贵其实是更符合逻辑的，因为被叫的成本要比主叫高。但是符合技术逻辑的事情却未必符合用户的逻辑，从用户的角度而言，这种计费方式就显得比较难以接受。作为被叫的时候用户是被动的，他接通这个电话的需求并没有他当主叫的时候那么迫切，很多时候甚至无法从电话号码上辨别到底是谁在 Call 他，这个电话应不应该接都不知道，那他漫游时作为被叫要承担比主叫更高的费用作为用户而言自然就很不可理解。这种用户心理也是导致漫游资费改革的主要诱因。至于为什么漫游的时候用户当被叫的成本要比主叫更高，我们会在后面的章节中详加叙述。

我们已经知道，商业的蜂窝通信系统需要在原有的点对点方式的无线通信系统上添加很多东西，以及进行复杂的控制与管理和资源调度。一场战斗需要找到一个突破口，撕开突破口然后快速向纵深推进从而分割和撕裂整条防线往往是赢得一场胜利的不二法宝。在学习新知识的时候，我们也要选择一个切入口，并由这个切入口把我们带向纵深。在本书中，作者想选择全球最成熟的 GSM 网络作为突破口，和大家一起对无线蜂窝通信网的整体构架和信令流程进行一番学习和探讨，在必要的时候也附带讨论其他网络如 WCDMA 的内容。如果你对 GSM 从基带到射频、从终端到基站控制器都已然成竹在胸，那么当你再学习 CDMA、WCDMA 的时候就不需要花费很大的力气了。

在章节的安排上，作者希望大家能够先对 GSM 网络的组成有个整体的认识，然后逐步了解空中接口和 Abis 接口、A 接口，把这些接口从物理层到网络层都走一遍。最后，我们来看看 GSM 网络的信令流程，信令流程对于任何一个蜂窝通信网而言都极为重要，

它不仅规定了通信网的运作流程，也是对网络进行分析的利器！

在本章中，作者希望循序渐进，首先对GSM网络组成进行一个整体的介绍，让大家对网络有一个整体的概念。这或许并不会太难，因为我们之前已经在第1章中对GSM的网络组成进行过一次“水煮”，希望博得大家轻松一笑后还能留点印象，以便作为本章内容的铺垫。在作完整体介绍后，作者打算对SIM卡、手机、BTS、BSC、MSC、VLR和HLR进行一一解读，在这些内容里面又将不可避免地牵扯到电台这种古老的点对点通信工具。原因作者在上面已经说过了，点对点的无线通信是通信的基础，蜂窝通信系统也是在此基础上发展而来的。

4.2 GSM系统的发展历史及技术规范

4.2.1 GSM发展的历史背景

在介绍GSM网络之前，我们先来了解一下GSM的发展历史。对于一个通信系统，了解它的发展轨迹总是没错的。历史能给人的启迪是:“它从何处来？”、“要往何处去？”。读史以明智，即使是技术史也是如此。

GSM 数字移动通信系统是由欧洲主要电信运营者和制造厂家组成的标准化委员会设计出来的，它是在蜂窝系统的基础上发展而成的。

蜂窝系统的概念和理论早在20世纪60年代就由美国贝尔实验室等提了出来，但其复杂的控制系统，尤其是实现移动台的控制，直到70年代随着半导体技术的成熟，大规模集成电路器件和微处理器技术的发展以及表面贴装工艺的广泛应用，才为蜂窝移动通信的实现提供了技术基础。直到1979年美国在芝加哥开通了第一个AMPS（先进的移动电话业务）模拟蜂窝系统，瑞典于1981年9月开通了NMT（Nordic移动电话）系统，接着英国开通了TACS系统，德国开通了C-450系统等，见表4.1。

表4.1　　1991年欧洲主要蜂窝系统

国　　家	系　　统	频带（MHz）	建立日期（年）	用户数（千户）
英国	TACS	900	1985	1 200
瑞典、挪威	NMT	450	1981	1 300
法国	Radiocom2000	450,900	1985	300
	NMT	450	1989	90
意大利	RTMS	450	1985	60
	TACS	900	1990	560



续表

国　　家	系　　统	频带（MHz）	建立日期（年）	用户数（千户）
德国	C-450	450	1985	600
瑞士	NMT	900	1987	180
奥地利	NMT	450	1984	60
	TACS	900	1990	60
西班牙	NMT	450	1982	60
	TACS	900	1990	60

蜂窝移动通信的出现可以说是移动通信的一次革命，其频率复用大大提高了频率利用率并增大了系统容量，网络的智能化实现了越区转接和漫游功能，扩大了用户的服务范围，但上述模拟系统有 4 大缺点：

（1）各系统间没有公共接口；

（2）很难开展数据承载业务；

（3）频谱利用率低，无法适应大容量的需求；

（4）安全保密性差，易被窃听，易做“假机”。

尤其是在欧洲系统间没有公共接口，相互之间不能漫游，给用户之间的通信带来了很大的不便。

GSM 数字移动通信系统史源于欧洲。早在 1982 年，欧洲已有几大模拟蜂窝移动系统在运营，例如北欧多国的 NMT（北欧移动电话）和英国的 TACS（全接入通信系统）以及西欧其他各国也提供移动业务。当时这些系统是国内系统，不可能在国外使用。为了方便全欧洲统一使用移动电话，需要一种公共系统，1982 年北欧国家向 CEPT（欧洲邮政和电信会议）提交了一份建议书，要求制定 900MHz 频段的公共欧洲电信业务规范。在这次大会上就成立了一个在欧洲电信标准化协会（ETSI）技术委员会下的“移动特别小组”（Group Special Mobile）简称“GSM”来制定有关的标准和建议书。

1986 年，在巴黎，该小组对欧洲各国及各公司经大量研究和实验后所提出的 8 个建议系统进行了现场实验。

1987 年 5 月，GSM 成员国就数字系统采用窄带时分多址（TDMA）、规则脉冲激励长期预测（RPE-LTP）话音编码和高斯滤波最小移频键控（GMSK）调制方式达成一致意见。同年，欧洲 17 个国家的运营者和管理者签署了谅解备忘录（MoU），相互之间达成履行规范的协议。与此同时还成立了 MoU 组织，致力于 GSM 标准的发展。

1990 年完成了 GSM900 的规范，共产生了大约 130 项全面建议书，不同建议书经分组而成为一套 12 系列。

1991 年在欧洲开通了第一个系统，同时 MoU 组织为该系统设计和注册了市场商标，

将 GSM 更名为“全球移动通信系统”（Globa1 System for Mobile communications），从此移动通信跨入了第二代数字移动通信系统。同年，移动特别小组还完成了制定 1 800MHz 频段的公共欧洲电信业务的规范，名为 DCS1800 系统。该系统与 GSM900 具有同样的基本功能特性，因而该规范只占 GSM 建议的很小一部分，仅将 GSM900 和 DCS1800 之间的差别加以描述，绝大部分二者是通用的，二系统均可通称为 GSM 系统。

1992 年大多数欧洲 GSM 运营商开始商用业务。到 1994 年 5 月已有 50 个 GSM 网在世界上运营，10 月总用户数已超过 400 万户，国际漫游用户每月呼叫次数超过 500 万次，用户平均增长超过 50%。

1993 年欧洲第一个 DCS1800 系统投入运营。到 1994 年已有 6 个运营商采用了该系统。

据 GSM 协会 2006 年发布的报告：“在 6 月 17～18 日这个周末，全球 GSM 手机用户数已突破 20 亿。213 个国家和地区的 690 家移动通信网络运营商使用的是 GSM 技术。”GSM 取得了巨大的成功。

就其发展趋势而言，目前世界上绝大多数国家的移动通信运营商选择了“GSM—GPRS—WCDMA”的发展道路。WCDMA 也是目前最成熟、最主流的第三代移动通信系统。

4.2.2　GSM 系统的技术规范

GSM 系统的技术规范中只对功能和接口制定了详细规范，并未对硬件作出规定。这样做的目的是尽可能减少对设计者的限制，又使各运营商有可能购买不同厂家的设备。

GSM 系统的技术规范共分 12 章，见表 4.2。

表 4.2　GSM 规范目录

01	概述
02	业务方面
03	网络方面
04	MS-BS 接口与协议
05	无线路径上的物理层
06	话音编码规范
07	MS 的终端适配器
08	BS-MSC 接口
09	网络互通
10	业务互通
11	设备和型号认可规范
12	操作和维护



这些系列规范都是由 ETSI 组建的不同工作组和专家组编写而成的。1988 年春天完成第一阶段标准的第 1 个版本，以支撑当时的投标活动。后来修改过几次，1990 年以后除了传真方面的规范外，其他很少作改动，1992 年年底基本冻结。第二阶段标准到 1993 年年底也基本完成了主要部分，并于 1994 年年底冻结。为了提高系统的性能，从 1994 年 6 月起又开始考虑第 2＋阶段的有关标准的定义，后并入第二阶段标准，并宣布还会有第三阶段的标准。实际上由于第三代移动通信系统的提出，已终止第三阶段标准。

为了保证 GSM 网络内现有的和将来的业务开展，在制定标准时必须考虑兼容性的要求。

4.3 GSM网络组成及接口

4.3.1　GSM 网络组成

我们在第 1 章中已经用“水煮”的方式介绍过 GSM 网络的组成，在本节中我们再对 GSM 网络的组成及各部分的功能进行一下简单的介绍。一套完整的蜂窝无线通信系统通常由交换子系统（NSS，Network Switched Subsystem）、基站子系统（BSS，Base Station Subsystem），移动台（MS，Mobile Station）以及操作维护中心（OMC，Operations & Maintenance Center）构成。

各子系统具体的组成如图 4.1 所示，NSS 包括移动业务交换中心（MSC）、访问位置寄存器（VLR）、归属位置寄存器（HLR）、鉴权中心（AuC）和移动设备识别寄存器（EIR）；BSS 包括基站控制器（BSC）和基站收发信机（BTS）。交换子系统和其他网络如 PSTN（Public Switched Telephone Network，公用电话交换网）、PLMN（Public Lands Mobile-communication Network，公用陆地移动通信网）之间一般都有接口。

下面先简单了解各部分的功能，具体的内容会在随后几节中进行介绍。

1. 移动台

移动台就是移动用户设备部分，它由两部分组成：移动终端（MS）和用户识别卡（SIM）。

移动终端就是“机”，它可完成话音编码、信道编码、信息加密、信息的调制和解调、信息的发射和接收等功能。

SIM 卡就是“身份卡”，它类似于我们现在所用的 IC 卡，因此也称作智能卡，存有认证用户身份所需的所有信息，并能执行一些与安全保密有关的重要信息，以防止非法

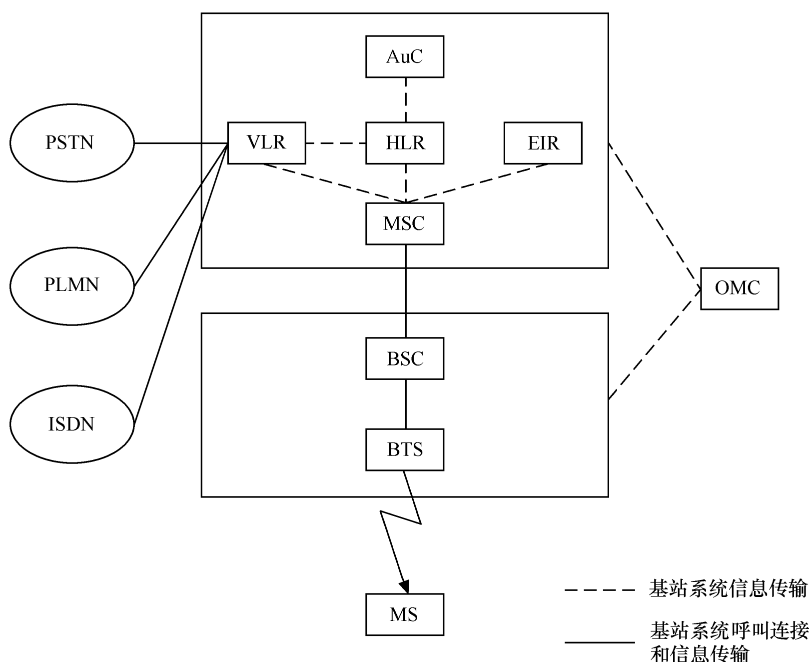


图 4.1　GSM 网络组成

用户进入网络。SIM 卡还存储与网络和用户有关的管理数据，只有插入 SIM 后移动终端才能接入进网，但 SIM 卡本身不是代金卡。

2. GSM 基站子系统（BSS）

BSS 是在一定的无线覆盖区中由 MSC 控制，与 MS 进行通信的系统设备，它主要负责完成无线发送/接收和无线资源管理等功能。功能实体可分为基站控制器（BSC）和基站收发信台（BTS）。

BSC：具有对一个或多个 BTS 进行控制的功能，它主要负责无线网络资源的管理、小区配置数据管理、功率控制、定位和切换等，是个很强的业务控制点。

BTS：无线接口设备，它完全由 BSC 控制，主要负责无线传输，完成无线与有线的转换、无线分集、无线信道加密、跳频等功能。

3. GSM 交换子系统（NSS）

NSS 主要完成交换功能和用户数据与移动性管理、安全性管理所需的数据库功能。NSS 由一系列功能实体所构成，各功能实体介绍如下。



（1）MSC：是 GSM 系统的核心，是对位于它所覆盖区域中的移动台进行控制和完成话路交换的功能实体，也是移动通信系统与其他公用通信网之间的接口。它可完成网络接口、公共信道信令系统和计费等功能，还可完成 BSS、MSC 之间的切换和辅助性的无线资源管理、移动性管理等。另外，为了建立至移动台的呼叫路由，每个 MS 还应能完成网关 MSC（GMSC）的功能，即查询位置信息的功能。

（2）VLR：是一个数据库，是存储 MSC 为了处理所管辖区域中 MS（统称拜访用户）的来话、去话呼叫所需检索的信息，例如用户的号码、所处位置区域的识别、向用户提供的服务等参数。

（3）HLR：也是一个数据库，是存储管理部门用于移动用户管理的数据。每个移动用户都应在其归属位置寄存器（HLR）注册登记，它主要存储两类信息：一是有关用户的参数；二是有关用户目前所处位置的信息，以便建立至移动台的呼叫路由，例如 MSC、VLR 地址等。

（4）AUC：用于产生为确定移动用户的身份和对呼叫保密所需鉴权、加密的三参数（随机号码 RAND、符号响应 SRES、密钥 Kc）的功能实体。

（5）EIR：也是一个数据库，存储有关移动台设备参数，主要完成对移动设备的识别、监视、闭锁等功能，以防止非法移动台的使用。

4. 操作维护中心（OMC）

GSM 系统还有个操作维护中心（OMC），它主要是对整个 GSM 网络进行管理和监控。通过它实现对 GSM 网内各种部件功能的监视、状态报告、故障诊断等功能。

4.3.2　“跑马圈地”与“免费搬迁”——Abis 接口引发的商业策略

为了各厂家的设备可以通用，上述各组成部分的连接都必须严格地符合接口标准，要不就无法实现通信。GSM 系统不仅对各个组成部分如 MSC 和 BSC 之间的接口定义明确，同样 GSM 规范对各接口所使用的分层协议也作了详细的定义。也就是说，不但定义了这个接口，这个接口之间交流信息的方式——也就是协议也被规定了。

我们左一个协议，右一个协议，“协议”到底是用来做什么的呢？通俗一点说，所谓协议，就是约定俗成的信息交流方式。人和人之间用来交流的语言就是人类的“协议”，机器和机器之间交流的语音也就是机器的“协议”。人类的“协议”有很多种，比如英语、汉语、日语、德语、法语、俄语等；机器的“协议”也有很多种，比如七号信令、一号信令等。人和人之间要交流，那么交流的双方就必须懂得一门共同的语言；机器和机器之间要交流，那么交流的双方就必须懂得一门共同的协议。

GSM 系统不同的接口采用的物理链路可能是不同的，每个接口都传递各自的消息，

完成各自的功能，这些都由相应的信令协议来实现。GSM 系统各接口采用的分层协议结构是符合开放系统互联（OSI）参考模型的。那么什么是 OSI 参考模型呢？我们会在第 7 章中进行详细的阐述。

分层的目的是为了让系统有一个清晰的分工，不同的分工归于不同的层次。那么各层的开发人员可以更好地专注于自己所在的领域，而不必考虑其他层的变动。图 4.2 展示了 GSM 系统中的不同接口。

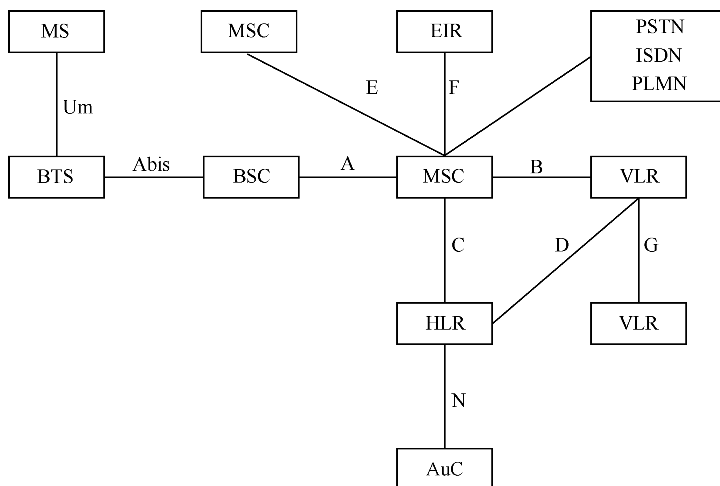


图 4.2 GSM 系统中的不同接口

在 GSM 系统中，BSC 与 MSC 之间的接口称为“A”接口、移动交换中心（MSC）与访问位置寄存器（VLR）之间的接口称为“B”接口、移动交换中心（MSC）与归属位置寄存器（HLR）之间的接口称为“C”接口、归属位置寄存器（HLR）与访问位置寄存器（VLR）之间的接口称为“D”接口、移动交换中心（MSC）与别的 MSC 之间的接口称为“E”接口、移动交换中心（MSC）与设备标志寄存器（EIR）之间的接口称为“F”接口、访问位置寄存器（VLR）之间的接口称为“G”接口、基站控制器（BSC）与基站收发信机（BTS）之间的接口称为“Abis”接口、基站收发信机（BTS）与移动台（MS）之间的接口称为“Um”接口。

相信上面一连串的各类接口已经让读者晕头转向了，其实没必要记这么多接口。有些接口甚至在国内干脆就没有用到，比如用于 MSC 和 EIR 交换信息的 F 接口，国内的几大运营商都是没有安装 EIR 的，自然也就无所谓 F 接口。

本书侧重的是无线通信，关注的是无线侧的内容，我们只需要了解从 MSC 至 MS 的接口，即 A 接口、Abis 接口和 Um 接口即可。后面章节对协议和信令的分析，也将围



绕这三大接口展开。

值得注意的是，GSM 规范中对 Abis 接口的协议并没有作详细的规定，不同的厂家都有自己的理解和定义，从而导致了不同厂家之间的 BSC 和 BTS 不能混用，比如说你不能在局房里安装华为的 BSC，基站里又安装爱立信的 BTS，它们所采用的协议可能有差别，从而导致无法完成通信。但 A 接口的规定是严格的，你完全可以安装摩托罗拉的 BSS 系统，然后采用北电的 MSC，两者之间可以并行不悖。

Abis 接口的独特之处导致了无线设备商独特的商务策略，即“跑马圈地”。全世界主流的设备商在运营商一期、二期购买无线设备的时候采取的商务策略基本是类似的，那就是低价抢地盘。对于设备商而言，这时候首先考虑的往往不是利润指标，其战略目标往往追求的是拿到更大的市场份额。一旦圈地完成了，一个地市采用了某个设备商的 BSC 和 BTS，由于 Abis 接口的协议具有不能通用的特殊属性，其他厂家的基站就再也无法插足其中。设备商前期圈地的微利润甚至负利润可以通过后期的升级、扩容、维保等长期收益来获得补偿。

Abis 接口的封闭特性阻碍了新兴设备商成长的步伐，为传统设备商的势力范围树立了一道天然的屏障。对于运营商而言，当然也希望看到更多的竞争，设备商划地为牢的局面对运营商而言是不利的。

GSM 标准的制定者显然看到了 Abis 接口的非开放特性对于整个产业链的影响，因此 3GPP 在 WCDMA 标准制定的时候就注意了对 Abis 接口的开放。当然，WCDMA 各接口的名称与 GSM 有所区别，但其架构基本一致。图 4.3 所示是 WCDMA 接口的示意图。

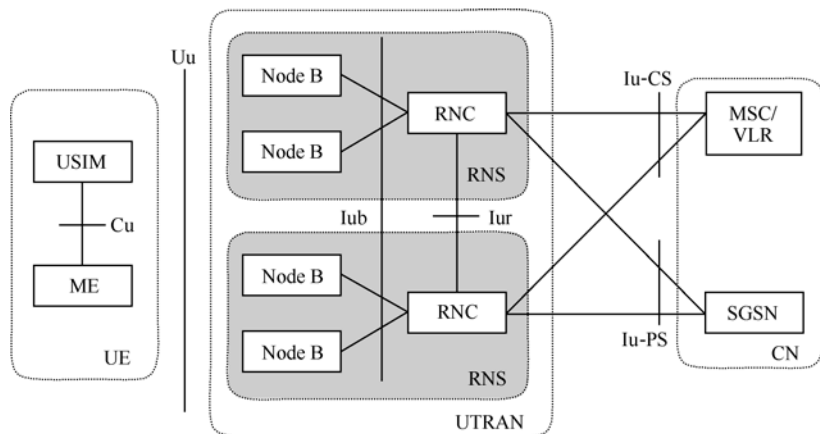


图 4.3　UTRAN 结构

在 WCDMA 系统中，UE 是 User Equipment 的意思，也就是用户设备，相当于 MS。

基站收发信机又称 Node B，相当于 BTS。Node B，这个名字很怪，至今有些学者和研究人员都搞不清这个词是怎么就突然冒出来的，算是一个莫名其妙就走红的词。无线网络控制器（RNC，Radio Network Controller）相当于 BSC。SGSN 属于分组域的东西，相当于 GPRS 网络中的 PCU，这里不对它展开讨论。

我们看到，原来的 Um 接口在 WCDMA 系统中被称为 Uu 接口，Abis 接口在 WCDMA 系统中被称为 Iub 接口，A 接口在 WCDMA 系统中被称为 Iu 接口。与 GSM 不同的是，这里的 Iub 接口是开放的，3GPP 希望通过 Iub 接口的开放引入更多竞争。还有人预言，在 3G 时代将有专门开发 Node B 的厂家出现。从理论上而言，Iub 接口既然开放了，那么专心致力于 Node B 的开发也就成为了一种可能，不过到目前为止还没有发现这样的趋势。

事实上，或许是惯性使然，“跑马圈地”的市场策略在 3G 时代并没有因为 Iub 接口的开放而得到改变，设备厂家争夺的焦点依然放在市场份额上。就拿 2008—2009 年中国三大运营商的 3G 设备招标来看，无论是媒体还是业内人士，每次开标其关注的焦点依然是市场份额，市场份额对于设备商来说依然是最重要的战略目标。运营商也暂时没有用不同厂家的 Node B 接入相同的 RNC 的习惯。

真正对“跑马圈地”这种商业模式构成致命杀伤力的是华为和中兴崛起后的“免费搬迁”策略。你不是圈了地让我在一块地方无法插手吗？那好，我就把你一个个地市整网替换掉，还是免费的，搬到别的地市当基站也好，当备件也罢，那我不管。既然无法从 Abis 接口入手分得一杯羹，就干脆把你一锅端了。在世界通信版图 2G 格局已经划定的情况下，“免费搬迁”策略被多个新兴设备商所采用，用于对抗传统设备商的“跑马圈地”策略。

4.4 移动信息专家——SIM卡

SIM 卡，是整个 GSM 系统中最小的部件，它的全称叫做 Subscriber Identification Module（用户识别模块）。SIM 卡的一个主要功能就是对移动电话用户进行身份验证，从而防止非法用户混进 GSM 网络。除了身份验证以外，它还存储了很多有用的信息，这些信息可以随着 SIM 卡被插入到任何一部手机上去用，实实在在算得上移动着的信息专家。



图 4.4 SIM 卡

相信很多人在营业厅都对这张卡有过不爽的情绪，一张不大的卡，补卡竟然收费 20 元，这也太贵了吧。

嘿嘿，还真别小看这张卡，这是一张 IC 卡，跟大学食



堂里的饭卡、水卡、机房上网卡等没有什么区别。丢了饭卡补卡要收费，丢了水卡补卡要收费，那么丢了 SIM 卡补卡自然也要收费喽。

上面的解释估计没有几个人能够服气，一张卡就是有一点点铜片，凭啥卖这个价？嗨嗨，这么想就大错特错了，你能想象这个铜片是带 CPU 的么？让我们来看看 SIM 卡的基本构成。

SIM 卡是通过卡面上的铜制接口来连接卡内逻辑电路与移动终端的，SIM 卡芯片有 8 个触点，通常与移动设备连接需要 6 个触点（取开手机的后盖看看手机的 SIM 卡卡槽就明白啦），具体接口定义如图 4.5 所示。

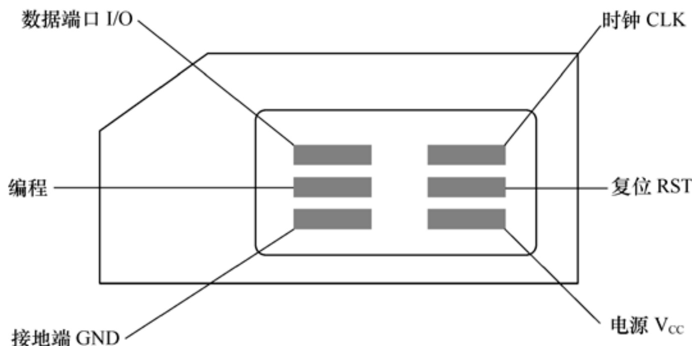


图 4.5　SIM 卡的接口图

扩充知识：SIM 卡是一个装有微处理器的芯片卡，它的内部有 5 个模块，并且每个模块都对应一个功能：微处理器 CPU（8bit）、程序存储器 ROM（3～8kbit）、工作存储器 RAM（6～16kbit），数据存储器 EEPROM（128～256kbit）和串行通信单元。这 5 个模块被胶封在 SIM 卡铜制接口后与普通 IC 卡封装方式相同。

对于 SIM 卡具体的电路组成与实现方式我们没必要深究，本篇的开篇语已经说过这不属于本书的内容，不去追究设备的物理实现并不妨碍我们对于 GSM 系统的深刻理解。

我们需要了解的是，一个物理设备是做什么的？为什么要这样设计？它与 GSM 系统中的其他设备有什么联系？从这样的角度来切入问题和理解问题，你会比机械地记忆一个知识点有更深刻的认识。

我们知道，手机有两大流派，一类是机卡一体的，像国外的 CDMA 手机以及国内早期的小灵通都是采取这种模式；另一类是机卡分离的，如 GSM 手机以及国内的 CDMA 手机都采用的这种方式。

机卡分离的初衷，就是为了将用户信息从手机中分离出来，由此就产生了 SIM 卡，电话、短信、用户信息都跟 SIM 卡走而不跟手机走，这多好。你可以买几部很炫的手机换着用，也可以和你的朋友随意地交换你们的智能手机玩，你可以今天玩 iPhone，明天玩

黑莓，后天再弄部 E71 假装商务人士，这多酷啊，机卡一体机就享受不到这样的好处喽。

既然 SIM 卡的初衷是为了将用户信息从手机中分离出来，那么 SIM 卡需要存储哪些用户信息呢？这是一个值得探讨的问题，现在请大家转换视角，从一个设计者的角度来思考这些问题。

首先，SIM 卡是有密码的，为什么需要密码呢？这张卡上面是有话费的对吧，那么丢了之后，你不希望一个陌生人捡了这张卡之后狂打电话，欠一大堆话费，然后被运营商的催缴大队来催账吧。于是，PIN 码应运而生（无数同学的 SIM 卡死于自己忘记了 PIN 码），PIN 码是个四位数，它有一个好处，就是你可以设置要用 SIM 卡必须输入 PIN 码，防止别人盗打你的电话。为了防止有些人实在过于执着，用无穷列举法破解你的 PIN 密码（就是从 0000 到 9999 一个个地试，试不出密码也要搞残废你的手机键盘），就设置了输错 3 次 PIN 码就锁卡，必须用运营商提供的 PUK 码才能解锁，PUK 码最多只能输入 10 次，超过 10 次这张卡就自动报废了。

PIN2 码和 PUK2 码的用法与上述 PIN 码和 PUK 码的用法基本一致，不过 PIN2 码和 PUK2 码是用于设置计费的，大家一般用不到。

总结：SIM 卡有 4 种密码：PIN 码、PUK 码、PIN2、PUK2 码。

密码设置完了，就该正儿八经考虑该存储些什么数据了。设计者把 SIM 卡看作一个 U 盘，下面设计了 3 个目录：根目录、GSM 应用目录和电信应用目录，如图 4.6 所示。

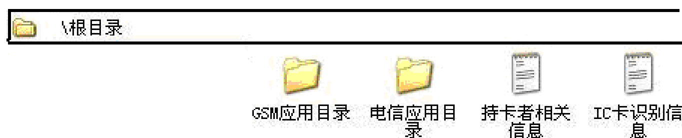


图 4.6　SIM 卡的根目录

根目录下包含了持卡者相关信息和 IC 卡识别信息，这个与本书没有什么关系，因此不作解释。

我们再看看电信应用目录下有什么，有手机号码、固定拨号数据、缩位拨号数据（也就是拨短号）、短信息存储数据以及其他一些数据（如图 4.7 所示），这些与我们想了解的东西也没有什么关系，不用理会。

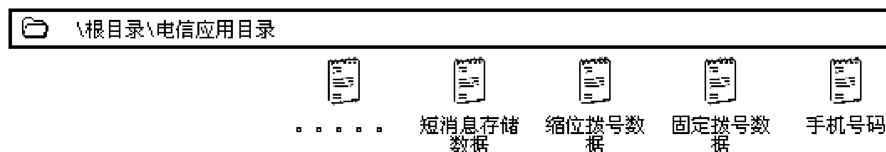


图 4.7　SIM 卡的电信应用目录



我们要关心的是 GSM 应用目录下的内容，这才是重点。大家知道，天底下没有免费的午餐，对于电信运营商来说更是如此。你抓起手机装上 SIM 卡开始打电话，运营商关心的第一个问题就是—老大，你这张卡不是伪造的吧？别我忙活了半天收不到钱哦！

为了说明你不是冒牌货，SIM 卡里需要存储几个数据：IMSI 号和 Ki 号。IMSI 号是 SIM 卡的编号（如图 4.8 所示），名字也很大气（International Mobile Subscriber Identity，国际移动用户识别码）。Ki 号是伴随 IMSI 号产生的，Ki 号和 A3、A5、A8 算法一样属于全球 GSM 运营商的特级机密，这几种算法都是不对外公开的，一旦公开了，沃达丰、ATT、中国移动这些 GSM 网络的运营商就麻烦大了。Ki 号通过 A3 算法得出一个数值用于鉴权，然后通过 A5 和 A8 算法加密。嘿嘿，你也不想你和女朋友聊悄悄话，别人直接在旁边架起无线电台偷听吧，所示说加密那是肯定要的。鉴权和加密都与这个 Ki 号有关，可见 Ki 号是多么的重要。



图 4.8　ICCID 号与 PUK（ICCID 号是 SIM 卡发行时的序号）

除了鉴权和加密的数据，运营商还得知道你在哪里，要不人家打电话怎么找得到你，于是就设计了一个“位置信息数据”，里面含有你所在的位置区域号（LAI）、TMSI 号、位置状态更新等信息。不知道什么叫 TMSI 号，什么叫位置状态更新没关系，后面我们会讲到。

除此之外，网络还经常告诉手机一些信息，手机把这些信息存储于 SIM 卡，叫做“BCCH 信息”。

GSM 应用目录下还有一些其他的内容，我们不再赘述。



图 4.9　SIM 卡的 GSM 应用目录

上面涉及的众多内容大家可能一时间还有些不熟悉、不理解，因为这与后面的一些内容息息相关，等我们学完信令流程，这些内容自然就变得很简单了。

SIM 卡总结如图 4.10 所示。

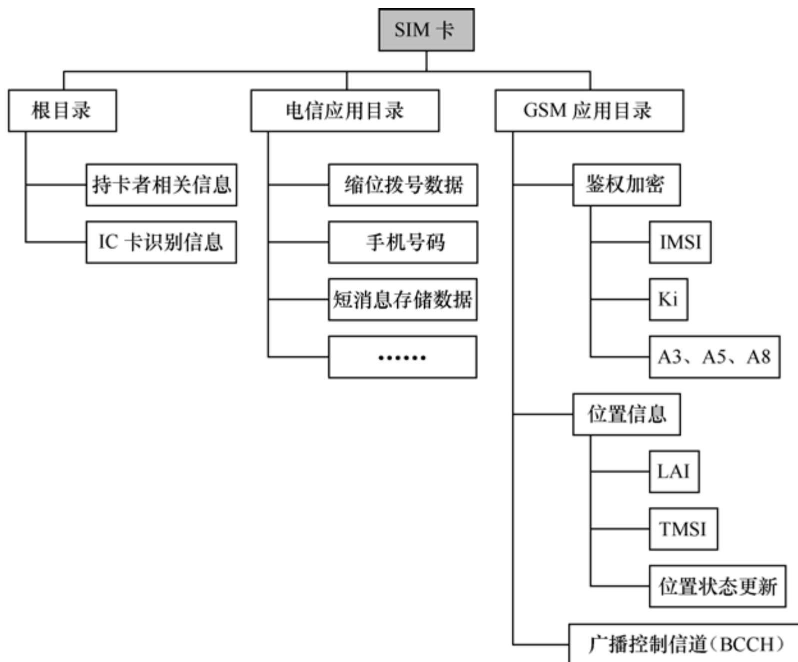


图 4.10　SIM 卡总结

4.5 从电台到基站——也谈手机与BTS

介绍完 SIM 卡以后，按理应该介绍手机了，因为这样显得比较循序渐进，有条有理。不过作者还是觉得，没有必要为手机单独开一节，因为手机的很多功能和 BTS（基站收发信机）很类似，我们不如把它们合在一起讲好了。

要了解 BTS，首先来谈谈电台吧。电台这种点对点的通信方式，比我们的无线蜂窝网络要简单得多，但是基本的骨架，如编码、调制、滤波等却一样都不少。从电台切入，有利于我们由浅入深地理解通信网络。

4.5.1　手机与点对点通信

图 4.11 和图 4.12 所示的是古老的电台和古老的步话机。





图 4.11　无线电台



图 4.12　最早使用的古老的步话机

看起来样子很丑，体积很大，一点也不如我们的手机乖巧。没办法啊，战地通信没人给你建网络，要完成长距离的点对点通信，发射功率就必须要大，要不然电磁波还没传送到对方就已经在空中衰减完了，那你就在阵地上听天由命吧。发射功率大，体积自然也就大，你总不能指望装在遥控器里的 5 号电池把信号从武汉传到南京吧。过了 10 米你再摁摁遥控器试试，看看电视机有反应没。图 4.13 为我们现在所使用的手机中的一种，看起来的确比那些笨重的电台和步话机要方便不少。



图 4.13　手机

话说我们已经讲了一大堆的理论，各位读者可能都觉得有点无聊了。光讲理论，什么时候能来点实际点的，不是说实践出真知嘛。那好，现在就是我们把这些理论落到实处的时候了，相信本书的很多读者还没有摸过真正的电信级通信设备，那我们就逛逛运营商的机房吧，抽出这块板子那块载频瞅一瞅，然后结合我们前面的理论看一看。或许这样，无论对于理论，还是实际的网络，我们都会有更深刻的认识。前面不是说过嘛，知识贵在联结，一个单独的知识点是没有太多价值的，你需要找到点与点之间的联系，这样建立的知识网才牢不可破。在理论与实践之间，你也需要找一根绳子，把它们栓起来，栓得紧紧地！

就手机和上面所述的电台以及步话机而言，它们之间并没有什么本质的区别，都是点对点的无线通信。这句话可能会引起争议，因为电台对电台、步话机对步话机的确是单点通信，而手机是蜂窝通信的一部分，它是存在于一张网络里的，并不是直接和另一



台手机完成通信。不过我们可以看到，手机每次通信的时候，只需要和它锁定的基站去交换信息，不需要去考虑网络是如何组成的，也不需要去考虑其他终端的情况，这些问题统统交给 BSS 侧乃至交换侧去考虑。在单次通信的时候，它的行为和电台实在没有多大的区别。既然如此，那么我们就通过介绍手机的工作原理来介绍点对点的通信，随后再来考虑一个蜂窝通信网需要增加什么内容。

图 4.13 所示的手机都能完成一些什么工作呢？答：打电话！晕，完全正确，但不是我们想要的答案。我们不妨来理一理手机的工作流程，这样有助于我们加深对知识的认识。（注：下文中假设该手机使用的是 GSM 网络）

手机的核心部件说简单也简单，就只有天线、射频、中频和基带四部分（显示屏、电池、键盘之类就不算在内了）；说复杂也真复杂，这些部件还个个都是些难缠的主，下面我们就来一一介绍这些部件。

1. 天线

天线是手机发射和接收电磁波的工具。比较老的手机都杵着一根天线，很是明显。而如今手机的天线一般都隐藏了，改为内置了。内置天线成为了当今的潮流，而诺基亚开始力推内置天线的时候却并不为业界所接受。很多工程师认为，手机怎么可以没有外置天线呢，太不可思议了，这还能叫手机吗？真理永远掌握在用户手中，这或许就是商品经济时代给予我们的启发。



图 4.14 手机天线

天线是手机接收信号的第一级电路，也是手机发射信号的最后一级电路。它主要有两个作用：一是将空中的电磁波转化为高频电流并将其输送到接收电路中（如图 4.14 所示），发射的时候则恰好相反，把高频电流转化为电磁波；二是分离发射信号与接收信号，避免二者之间互相干扰，我们在 3.2.5 节中说过，GSM 收与发有 3 个时隙的时间差，发射机和接收机都是间歇性工作的。那么要完成这项功能就简单了，我们只需要通过逻辑电路控制天线开关，让它在适当的时隙接入发射机或者接收机通道，这个问题就解决了。

2. 低噪声放大电路

咱得注意一点，从天线感应到的信号是非常微弱的，我们得把这个信号放大，要不后面的工作就非常麻烦。其实它还有另一层作用，也就是为接下来的混频提供必要的信号强度。

在手机电路图中，这个原器件叫做 LNA（Low Noise Amplifier，低噪声放大器），这个器件通常置于天线电路之后，用于放大信号。



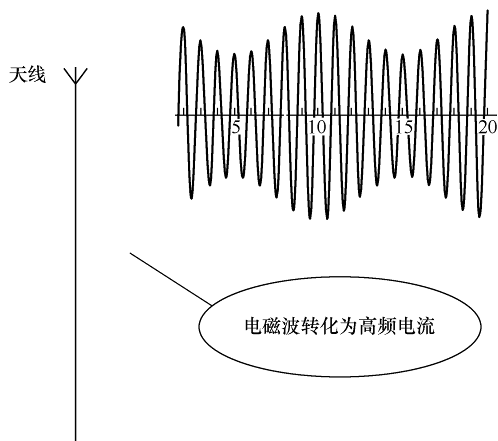


图 4.15　天线的作用

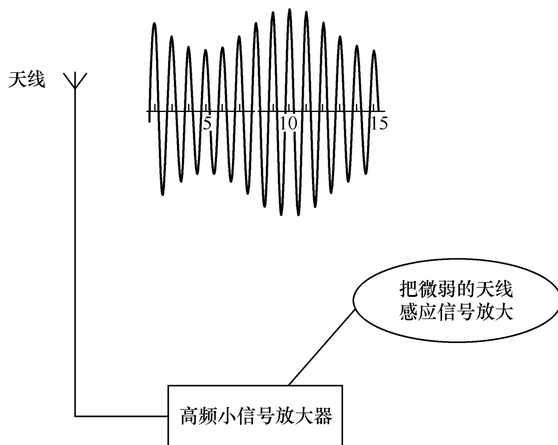


图 4.16　低噪声放大电路

3. 射频滤波器

请注意，我们的手机天线接收的信号可不止是 GSM900 所在频段的信号，它还完全可能接收到其他频段的信号。比如比它频率更高的信号，它也完全可以接收。问题是那些信号对咱没用，咱留它作甚，因此需要一个射频滤波器，对 GSM 接收频段以外的信号通通过滤掉。

4. 超外差电路

对于超外差这个名词，相信大家已经比较熟悉了。因为我们的收音机往往都是超外差制式的，从各种各样的无线电杂志上我们也常常可以看到这个名词。

不过我们虽然对这个名词熟悉，但估计还是有很多人并不清楚超外差的真正含义，这个超外差到底是干嘛的，有这个必要吗？

所谓超外差电路，就是把高频电流信号降下来变成中频电流信号，然后进行放大和选频的电路。之所以不在高频直接进行放大和选频，是因为要制作一个频率可变且增益高、工作频率也高的放大器，其技术难度和造价都远远高于中频。

那么怎样实现由高频到中频的转换呢？在实际操作过程中，我们是通过混频器来实现的，混频器一般和本机的振荡器结合使用。本机振荡器产生一个大小为 f_L 的频率，假设高频信号的频率为 f_S，那么我们就可以设置一个合适的 f_L，使得 $f_I=f_L-f_S$。这里的 f_I 指的就是中频，如果 f_S 发生变化，那么我们就相应地改变本地振荡器产生的 f_L 的频率，使得中频 f_I 总是为一个固定的频率，这样一来中频这部分的电路元件其工作频率就不需要变化，自然好设计得多，如图 4.18 所示。



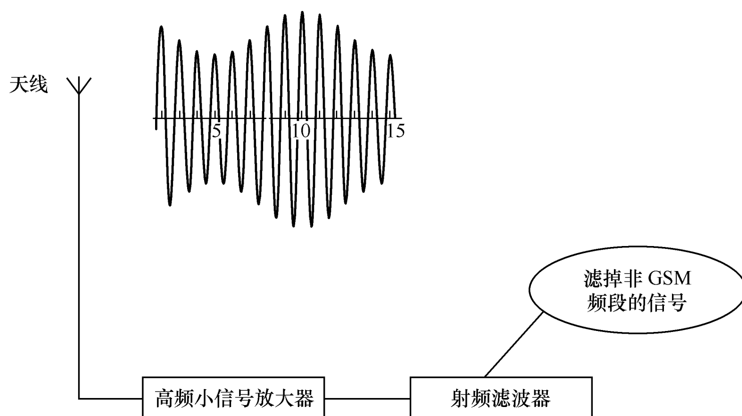


图 4.17　射频滤波器的作用

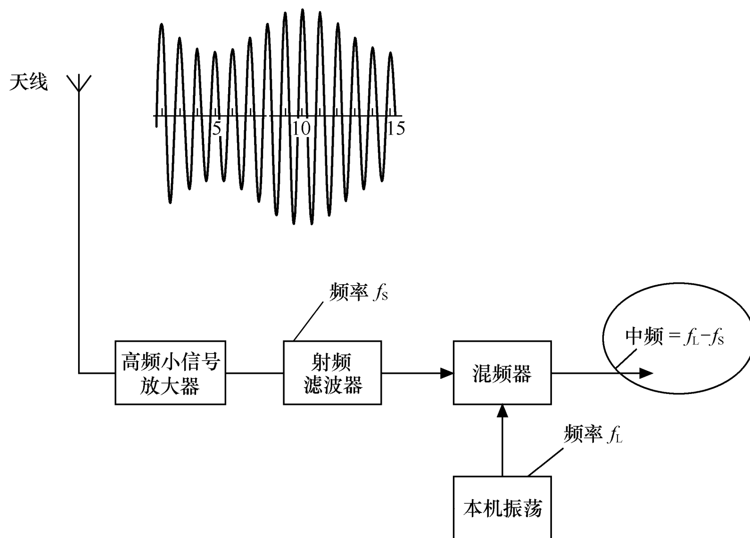


图 4.18　混频器的作用——产生固定的中频

产生一个固定的中频后，我们需要对这个中频信号进行放大，而且是通过多级调谐器进行放大。因为手机放大器的总增益要达到 120dB，不进行多级放大不行啊。放大完成之后，就应该解调了，我们要把射频信号还原为基带信号，如图 4.19 所示。这个过程还真够复杂的！

以上我们所说的是手机的射频和中频部分，而基带信号的处理通常被认为是手机最核心和技术含量最高的部分。掌握了基带芯片技术的厂家屈指可数，其中德州仪器（主要供应诺基亚和索尼爱立信）、飞思卡尔（主要供应摩托罗拉）、联发科（主要供应中国大陆厂家）、ADI（主要供应 LG 和夏普）、高通（CDMA 基频霸主，市场占有率超过 80%），算是基带芯片技术厂家的佼佼者。



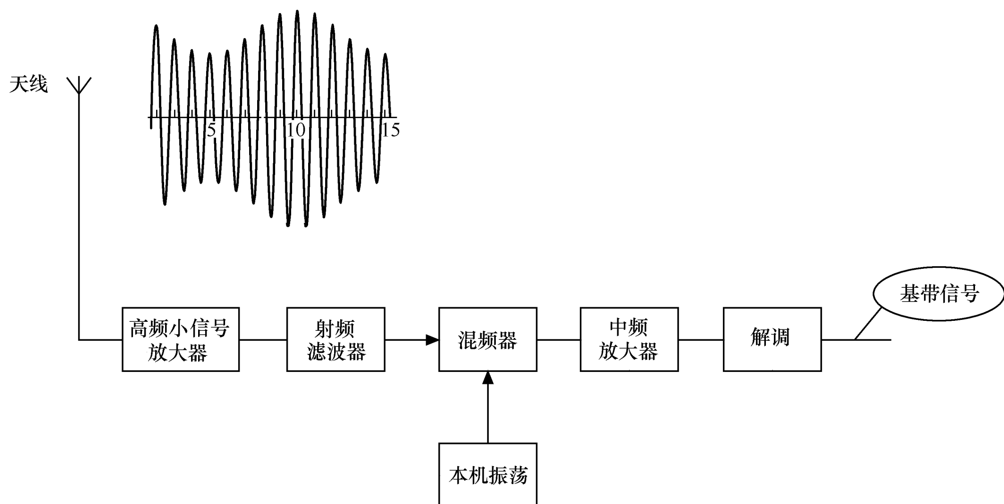


图 4.19　解调后产生基带信号

话先说到这里，那么基带芯片又包含哪些功能呢？模拟基带信号首先要进行 GMSK 解调，以实现从模拟到数字的转换。对于 GMSK 调制，是调制的一种，请参见第 2 章。

完成了从模拟到数字的转换后，我们需要在 DSP 电路中对数字信号进行解密，我们将在第 8 章介绍 GSM 的加密方式，这里只需要知道 GSM 是通过 A8 算法加密的。那么得到数字信号之后，我们显然需要先进行解密才能进行其他的工作。就好比电台的发报员收到一份电报，先得用密码本把电报解密了才能进行其他的处理。

对数字信号进行解密后，我们还得对信号进行去交织。我们在 3.2.2 节中介绍过，数字信号在发射前是要进行交织的，以避免碰到小尺度衰落或者突发噪声从而损失过多的连续信息导致信号无法通过信道编码等手段来恢复。块与块在发射的时候交叉了，那么在接收的时候就要把它归位到原来的位置，这就是去交织。

去交织后，还需要进行信道解码。我们都知道，空中的无线信道其性能是很糟糕的，需要填充大量的冗余信息用来作为纠错信息才能保证有效地传送信号。那么在还原的时候，自然要进行信道解码，将这些冗余位去掉。

接下来就是语音解码，将数字信号还原为 64kbit/s 的 PCM 编码，最后由该编码产生模拟语音信号，经音频放大后驱动听筒发声。

我们上文所述的从射频、中频到基带的处理，这么多芯片全部都集成在图 4.20 所示的小小的电路板上，工艺不可谓不复杂，技术含量不可谓不高。中国目前已经成为世界上最大的手机生产基地和出口基地，但是在基带等核心芯片上的水准与世界一流企业仍有较大差距。由于技术实力上的差距，目前国内终端的高端市场被诺基亚、三星、索尼爱立信等国际大企业牢牢把持住，而低端市场又被采用联发科 TURNKEY 方



案的众多山寨厂家所盘踞。国内的很多手机厂家不得不在高端与低端的上下挤压下艰难求生存。我们都希望在国内的这些终端制造商中能诞生像华为、中兴一样能掌握核心技术，能够真正和国外一流企业进行竞争的公司，那么中华民族的电信强国之梦，就会实现得更快。

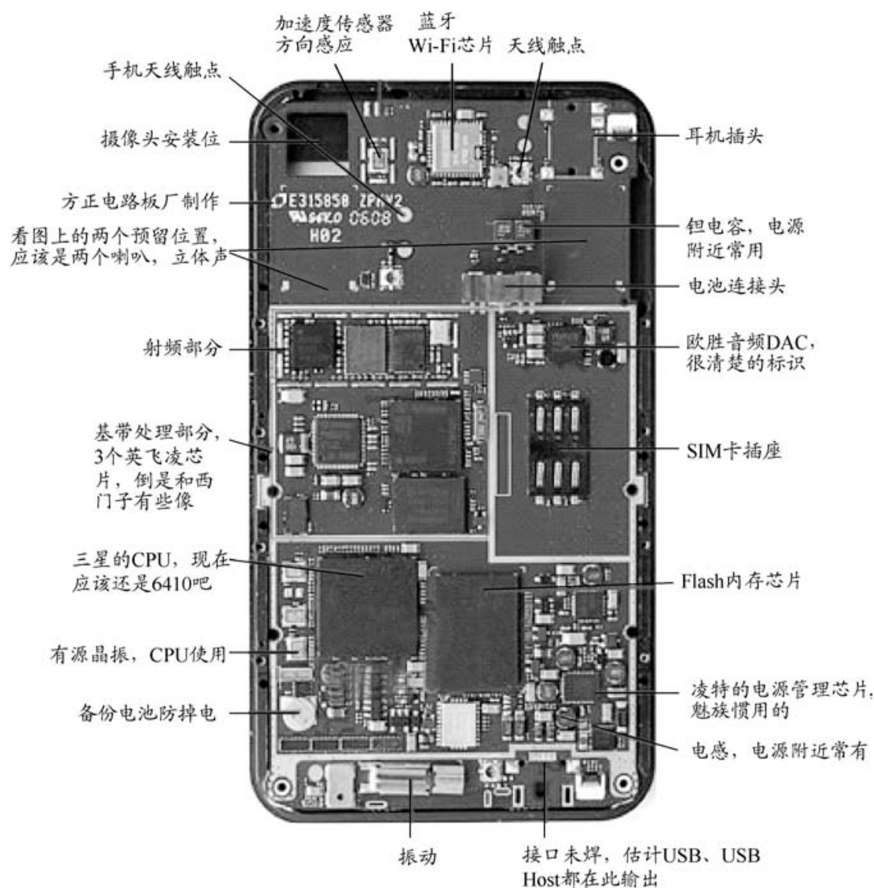


图 4.20　魅族 M8 的电路板

4.5.2　劳模 CTU 和它的团队——BTS

在本小节中，作者不打算像介绍手机组成一样来描述电路，因为厂家与厂家之间的电路实现或许会有很大不同。在这里，笔者也只能用“或许”二字而已，因为基站收发信机的电路都属于各厂家的保密内容，外人一般是拿不到的，即使能拿到，对于不做这块研发的人而言，也没有什么价值。本书的目的是希望大家可以掌握 GSM 系统的工作原理，对于 BTS 和 BSC 这些极为复杂的设备，我们了解到板件即可。



我们前面说了，手机和基站收发信机很多时候的工作都类似于一个电台。电台需要完成的工作有“语音编码、语音解码、信道编码、信道解码、交织、去交织、调制、解调、加密、解密、功率放大等等”，这些内容我们在介绍手机的工作流程时都讲过。在 BTS 中，这些工作都由载频来完成。载频的英文说法各厂家并不一致，摩托罗拉称之为 CTU（Compact Transceiver Unit，紧凑型收发单元），而爱立信则称之为 TRU（Transmisson Receiver Unit，收发单元）。图 4.21 为摩托罗拉的载频。



图 4.21　摩托罗拉的第二代载频

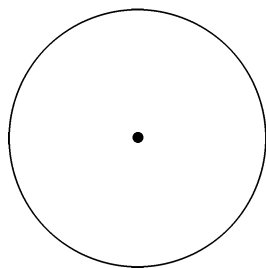
然而仅上述所说的数字处理的内容对于载频而言并不够，它还需要完成 GSM 系统赋予它的一些工作。GSM 是一个 TDMA 系统，为了避免多径效应导致的码间干扰，还应当进行均衡处理，这是 3.2.5 节的内容；对于任何一个蜂窝通信系统，为了尽量降低终端与终端之间的干扰，功率控制都是必不可少的，GSM 自然也不例外，这是 3.3.1 节的内容，对于蜂窝系统而言，为了保障用户连续不间断地通话，切换也是必须的。无论是功率控制也好，切换控制也罢，BTS 都必须向 BSC 出具一份测量报告，BSC 才好作出判读。那么很不幸，作为与手机联系最紧密的伙计，监视信号强度的任务也不可避免地落到了它头上；我们玩电台或者收音机的时候，它的工作频率往往是我们手动调谐上去的，GSM 都是数字通信系统了，自然不能干这么没创意的事情，载频上可设安装旋钮来调整它的工作频率，网络管理系统让它在哪个频率上工作，它就自动调谐到这个频率上去。所以 CTU 的功能就加上了生成执行发射和接收功能所需的 RF 频率。既然生成频率的工作交给你了，那么跳频的工作你也没得跑，这是 3.2.3 节中提到的内容；最后，兄弟，你既然这么能干，那么测试天馈驻波比（VSWR）的工作也交给你好不好啊？

载频一个趔趄晕翻在地，口吐白沫，再也没有起来，立即送至医院抢救，诊断结果为：“过劳死”。下面我们就来看看这位英勇无畏、任劳任怨的劳模兄弟——载频的模样（图 4.21 所示）。



话说这位劳模还是很值钱的，设备商卖无线设备都是以载频计价的，因为载频直接决定了设备能够支持的最大通话用户数，而其余设备如机柜等都是不计价的，这也是电信设备与其他商品的不同之处。其他所有设备的费用都折价算在载频里，这也就造成了载频价格的高昂。

劳模算是红花了，红花还得绿叶衬啊，一个好汉还得三个帮不是。无线信号处理的活基本被它干完了，但除此之外，还有不少别的活要干呢。话说在手机和电台中都有的那位天线兄弟，你去哪里了呢，你不干活，谁来接收电磁波啊？别急，天线是少不了的，BTS 和手机在这方面无二致，天线都是接收信号的第一道门和发射信号的最后一道门。天线分为全向天线和定向天线两种，全向站是指整个基站只有一个小区，进行 360° 范围的覆盖，而定向站则把整个基站分为 3 个小区，每个小区只覆盖其中 120° 的范围，3 个小区一起完成 360° 的覆盖。图 4.22 描述了全向天线和定向天线覆盖方式的不同。



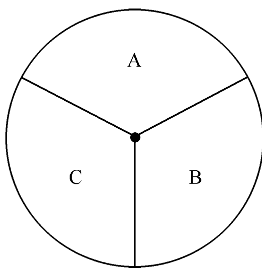


图 4.22　全向站与定向站

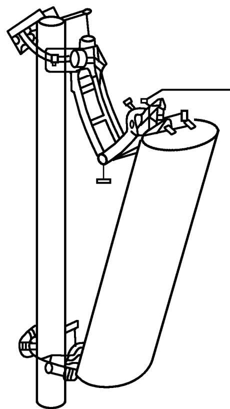


图 4.23　无线

好，我们总算搞定了一片绿叶，不过对于构架一个完整的通信系统，这还不够。我们回想一下，手机天线之后紧跟的电路是什么——是低噪声放大器和 RF 滤波器（把不属于 GSM900 的电磁波滤掉），在 BTS 中承担这项工作的往往是双工器。呃，你的名字叫做双工器，你怎么能只干放大和滤波的活呢，这电磁波的收与发都在这一根天线上，谁来保障它们可以并行不悖地工作，井水不犯河水呢，双工器你责无旁贷。另外，你说你离天馈线这么近，天馈的电压驻波比你得测量吧，要不怎么说“近水楼台先得月”呢，啥，你说你数学不好，不会计算驻波比 VSWR？谁让你计算了，你把这些电压测量一下记录下来，然后发给 CTU 去算不就结了呗，难道这也不会啊。

我们看到了，双工器的主要工作就是保障收发的分开。那么就还有一块有点类似的工作没有人做，什么工作呢？我们知道，一个扇区通常只有一根天线，但通常都不止一块载频，也就是说，不同载频的电磁信号要在同一根天线上运行，谁来区分它们呢？换句话说，



谁来完成来自不同载频信号的合路与分解呢？嗯，这个岗位不能没人干，我们还需要招一个新员工，这位老兄就是合路器了。这位老兄主要的工作和邮局里的邮寄员没有什么两样，每天上班就是把来自载频的信件（信号）收拢到一起，打一个包送给天线，天线送来的包裹呢，拆开分拣给各个载频。哼哼，你就干这么点活，你说你怎么可能有劳模值钱！

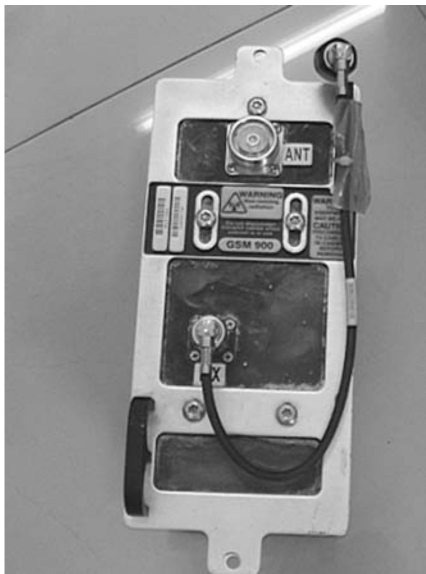


图 4.24　双工器

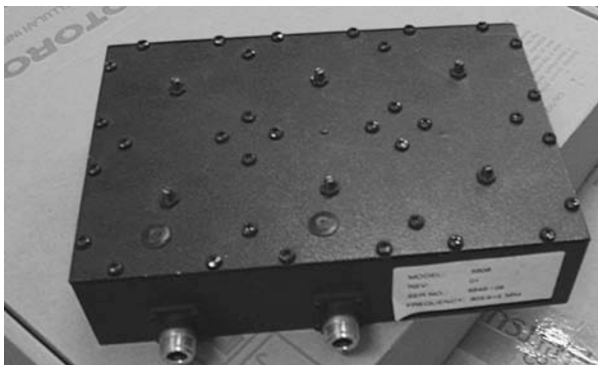


图 4.25　合路器

话说 CTU、天线、双工器、合路器，有收有发，有合路有分解，滤波放大数字信号处理一样不少，团队算是整整齐齐的。电台老兄前来参观，哈喇子都直流，爽呆了啊，我一个人干的活你们这么多人干，这时代果然进步了啊，可以多拿钱少干活！

CTU 听到电台的夸奖，自然是踌躇满志，俺这里干啥活的都有，分工明晰，人员齐整，是该去 GSM 总部申请个“最佳团队”奖了吧。

CTU 自信满满地来到了总部，没想到被总部劈头盖脸臭骂了一顿回来了：“我说 CTU 同学，你是不是想搞分裂啊。你忘了电信网络必须是一张全程全网的网络么。哦，你那里是啥人都不缺了，你那一亩三分地耕得好好的。谁来和其他团队联系？谁来接收你的上级 BSC 的指示并向它反馈和汇报情况？谁来对你整个团队进行调度和控制？”

一连串的连珠炮般的追问把 CTU 给问傻了，CTU 最擅长的工作是“把信送给加西亚”（注：“把信送给加西亚”是一个传奇故事。一位名叫罗文的英雄接到麦金莱总统的任务——给加西亚将军送一封决定战争命运的信，他没有任何推诿，而是以其绝对的忠诚、责任感和创造奇迹的主动性完成了这件“不可能完成的任务”）。执行力强是它的强项，工作再多再累也从不叫苦。可是遇到什么管理啊、调度啊、控制啊、沟通啊这些复杂的

管理学范畴的内容就傻眼了，没办法啊，CTU 是工科出身，整个一工程师思维，至今也没个时间读个 MBA，不能在这方面对他要求太多。

经高人点拨，CTU 决定去耶鲁大学聘请一个 MBA 来担任总经理，这位品学兼优的同学名叫主控板。主控板同学聪明啊，它上任的第一件事情就是修复和上级 BSC 的关系，这 Abis 接口的通信好久都不畅了，俺去疏通疏通。

Abis 接口疏通了，BSC 的脸色也终于阴转晴了："啥叫全程全网，Abis 接口都不要了，BTS 和 BSC 都不通信了，这还了得，这还能叫电信网吗？CTU 啊 CTU，你要有人家主控板一半聪明，也不至于……"。

作为一个垂直管理的连锁式企业，标准化是必须的。既然 Abis 接口通了，BSC 就决定得干点什么。它首先要求人力资源部搞了一个 CM 数据库（Configuration Management Database），这数据库干嘛用呢，当然是写企划书和岗位说明书了。就岗位说明书而言，一个分公司该配几个主控板（安排几个副总也是常有的嘛），几块载频，载频该配置哪些频点都清清楚楚；就企划书而言，分公司办公楼的规格（机柜类型），分公司的全球识别号（CGI）、位置区标识（LAI）等等一样都不能少。有些分公司有些小调皮，故意玩下失踪（掉电重启）就想把 BSC 的种种要求抛之脑后（数据丢失），BSC 这时就会不急不慌地把数据库翻出来："嗨，你那里的记录我这里都清清楚楚呢，还是照章办事吧"。

事还没完，现在虽然是主控板当总经理了，但是 BSC 仍然有点喜欢越级指挥，常常有指令要发给载频。主控板夹在中间很不是滋味，经常是接到上级的命令，拆开一看是给载频的。主控板也是机灵，安排综合部买了一堆叫 TEI（Terminal Endpoint Identifier，终端点标识）的标签送给了 BSC。以后 BSC 下发的指令，都在上面贴个 TEI 的标签，红色的就是找自己的，蓝色的就是找载频的，主控板看见贴着蓝色标签的命令就直接扔给载频，所谓眼不见心不烦嘛。

解决了和上级之间的矛盾以后，主控板这位 CEO 着手理清内部的头绪。不愧是耶鲁大学的高材生，主控板同学很快就发现公司内部问题多多，矛盾重重，远不如 CTU 去 GSM 总部时所说的那么一团和谐。

首先是公司内部居然没有一个统一的时钟，主控板、载频、双工器这些人每人都有自己的手表。有的人为了迟到把表拨慢一点，有的人为了早退把表拨快一点，谁和谁的时间都不一致，工作的时间完全匹配不上，经常把用户要传达的信息送错。主控板忍无可忍了，直接给人力资源部经理拨了一个电话："听好了，下面我说的事情不办好你就可以下岗了！GSM 系统本来就是一个时分复用系统，现在连时间都不统一了，我还玩个锤子啊。你去发个通知，所有人从明天开始不得再戴手表。然后去买个直径一米的电子钟，挂在公司大门的墙壁上，买它百十根数据线，一头连电子钟，另一头连各个办公室的显示终端，这些数据线就叫时间总线，大家的时间必须统一，要不这工作没法开展了。"



话说当年 CTU 主政时代，没有谁管理谁，也没有谁控制谁。这公司内部各忙各的，连条沟通渠道都没有。主控板召开了一次公司会议，畅谈了建设公司沟通渠道的重要性和必要性。在 CEO 的大力推动下，这条总线终于建立起来了，就称为本地总线（Local Bus），用于主控板、载频等设备之间的沟通。

我们知道 GSM 有一项重要的工作称为跳频，在 3.2.3 节中有描述。基带跳频的话自然要把信号以一个时隙为基础送至不同的载频。载频何许人也，都是一些精明强干的角色，各负责自己那一亩三分地，谁也不想跟谁扯上关系，想让他们互相合作不磕磕碰碰，咳咳，一个字，难！这时候，主控板良好的专业素质帮了他，科特勒的《营销管理》他是读得滚瓜烂熟的，像这种扯皮的事情也不难处理，就是成立一个高于它们的跨职能小组来统一协调这些事情即可。所以主控板又成立了一条 X 总线，用于处理基带跳频业务。

到这个时候，BTS 的体系架构终于流畅地运转起来，主控板开始悠闲地坐在沙发上，品茗着绿茶，盘算什么时候去 GSM 总部申请奖励……

4.6 计算机与通信的交融——BSC

很多时候，通信专业都是被划在 EE（Electronic Engineering，电子工程）中的，随着计算机技术与通信技术的逐渐融合与交叉，一些学校也开始尝试将其划到 CS（Computer Science，计算机科学）中。在 BSC 的架构中，我们看到了太多属于计算机思维层面的东西，比如说总线、处理器、DRAM、SRAM、EEPROM、令牌环。或者说，BSC 干脆就是一个大型的计算机，一个用于通信的大型计算机。

4.6.1 总线的概念

对于一个复杂的事务，需要一条线索将其串连起来，才能井井有条，使人不至于毫无头绪。就比如小说，一般都要有一条明线、一条暗线，脉络若不清晰，读者是很难分清人物和事件的。

对于 BSC 这么一个复杂的庞然大物，它的组成部分是如此之多，每个部分的功能与构造也是极为复杂的。如果没有一条主线将其串联起来，那么学习起来是非常麻烦的。在本节中，作者试图以总线来串联起 BSC 的众多器件。介绍 BSC 的时候作者将以摩托罗拉的 BSC 作为主体，兼带介绍华为的 BSS6.1 系列。不同厂家的 BSC 差别是很大的，但是其架构是基本一致的，因为 BSC 要承担的工作都是基本相同的。所以理解了一个厂家的 BSC，再去学习其他厂家的 BSC，其基本理念和思想是可以移植过来的，学起来并不会困难。

1. 总线的由来

总线的来历其实很简单，我们想象一下，对于计算机或者 BSC 这么一个复杂的设备而言，如果它的各个组成部分都采取一一相连的方式来完成彼此间的通信的话，那么资源的浪费一定相当可怕，如图 4.26 所示。

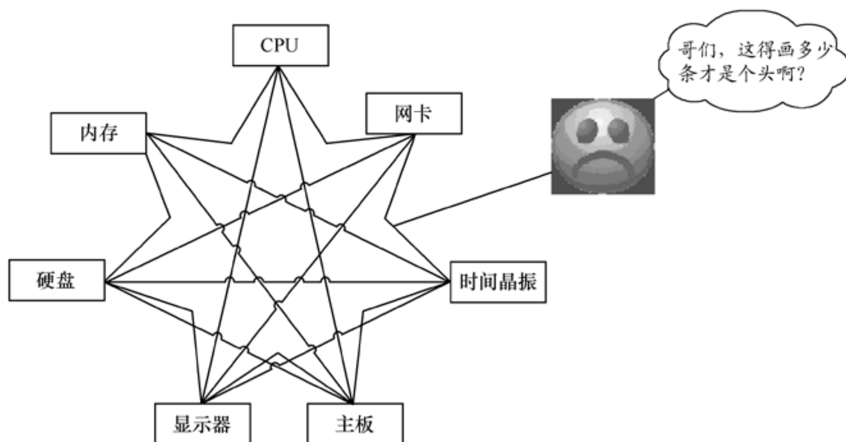


图 4.26　直接相连的方式

很多时候，其实通信与交通有其内在的相通之处：通信的目的，在于将信息从一个地方传送到另一个地方：交通的目的，在于将物体从一个地方搬运到另一个地方。本质相近，承载的东西有所不同。

对于图 4.26 中所遇到的困惑，交通这个层面也会遇到，比如说要实现全国物流一盘棋，我是不是需要把每两个城市都用公路或者铁路连起来呢？答案是显然不需要，比如铁路，我们就建两条干线，就像“京广线”和“京九线”这样贯穿南北的大动脉，然后把其他城市通过支路连接到干线上就可以了。在计算机或者通信上，我们也有类似的思路，有很多设备需要通信，我们也需要一条动脉把设备串联起来，那就是“总线”。

2. 总线的简介

总线（BUS）是连接两个或多个通信设备的通信通路，如图 4.27 所示。

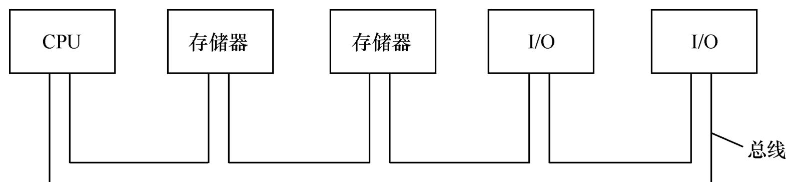


图 4.27　总线的雏形



这根雏形的总线我们也常称为数据总线。典型的数据总线包含 8、16 或 32 根线，这些线的数目称为数据总线的宽度。因为每条线每次传送 1 位，所以线的数目决定了每次可以同时传送多少位。数据总线的宽度是决定系统总体性能的关键因素。例如，如果数据总线为 8 位，而每条指令长 16 位，那么每个指令周期必须访问存储器模块两次。

我们现在需要思考一个问题，这些存储设备光有一根总线就够了吗？总线的特征是共享传输介质，多种设备都连在总线上，一个设备发出的信号可以被其他所有连接到总线上的设备所接收。如果两个设备同时发送，那么它们的信号将会重叠，这样就会产生混淆。因此，每次只能有一个设备成功地利用总线发送数据。那么某个时间谁可以发送这个信号，我们需要仲裁。这就需要增加一条控制总线来控制这些器件发送信号的行为，如图 4.28 所示。

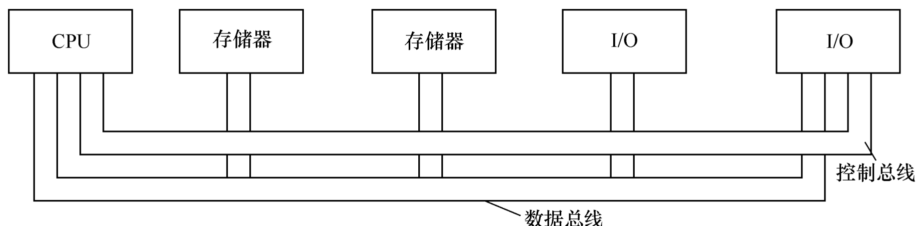


图 4.28　增加了控制总线的结构

话说有了数据总线并不代表万事大吉，我们还有一个问题没有解决。那就是信号“自何处来”、“往何处去”的问题，听起来有点像个哲学命题。也就是说，各块板件没有一个地址，信号该送到哪里去？不知道。

为此，我们需要添加一根地址总线，整体的架构这才算完整，如图 4.29 所示。

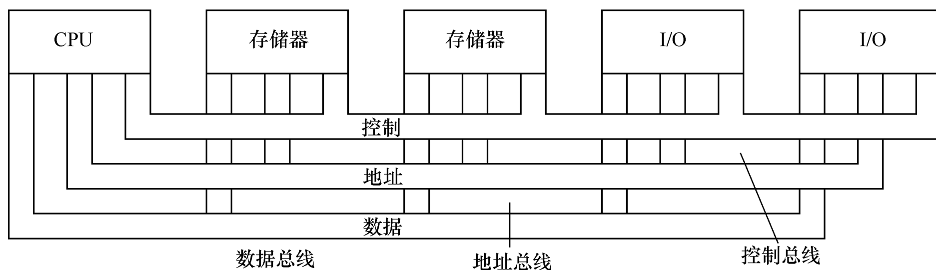


图 4.29　完整版的总线架构

总线的操作如下，如果一个模块希望向另一个模块发送数据，它必须做两件事：

（1）获得总线的使用权；

（2）通过总线传递数据。

如果一个模块希望向另一个模块请求数据，它也必须做两件事：

（1）获得总线的控制权；

（2）通过适当的控制线和地址线向另一个模块发送请求，然后它必须等待另一个模块发送数据。

从物理上讲，系统总线实际上是多条平行的导线。这些导线是在卡或板上蚀刻出来的金属线。总线延伸至所有的系统部件，每一个系统部件都连接了总线的全部或部分线。

4.6.2 BSC 中的总线

话说当年模拟通信时代，是没有什么 BSC 的，一个移动交换中心（MSC，Mobile Switching Center）就搞定了所有的事情。频率的分配也好，切换算法的判决和话务量的监控也罢，通通不需要别人插手。是啊，往往一个城市总共才几千门到上万门的容量，能有多复杂，再搞几个打杂的来不是浪费人力物力财力么。

到了数字通信时代，情况就完全不同了，一是新增了许多功能，比如什么编码、解码、卷积、交织、加密、采样时间提前量、功率控制，看得 MSC 头都大了，这可都是技术活，而且跟它原来的专业没多少关系，都推给它做它可做不来。另外，这用户数量是呈几何增长啊，工作的复杂程度也成倍增加。这么多工作，得有人分担分担压力啊。MSC 于是找了一个伙计来分担无线管理的功能以及一部分交换的功能，这个伙计就是 BSC（Base Station Controller，基站控制器）。

1. BSC 主要功能

BSC 的功能是为 BSS 提供全面控制。它控制并管理着相关的 BTS，并与操作和维护中心（OMC）以及移动交换中心（MSC）存在接口以便于完成之间的通信。BSC 的主要功能实体包含以下几部分。

（1）动态交换

在呼叫建立的过程中，MS 接到指令去使用空中接口的特定时隙发送和接收话务突发序列。信道配置由 BSC 的 GSM 话务处理软件进行。然而，呼叫的建立不仅仅需要一个空中接口信道，还需要一个陆地电路（Abis 接口电路和 A 接口电路）把它连接到 MSC。这个电路分配由 MSC 来做。交换的功能就是把每个 BSC 配置的信道与正确的 MSC 配置的电路连接起来。

这是在每个呼叫建立时发生的，是动态的、随机的，因此交换也只能是在动态的基础上进行，因为总是有呼叫开始和结束，呼叫结束了资源就应该释放，否则就会造成资源的浪费。在 BSC 中，是通过交换矩阵来完成这个功能的，所以说 BSC 内部的切换是不用惊动 MSC 的。手机在 BSC 所属的小区之间进行切换，BSC 通过内部交换时隙和端口就可以完成，A 接口的电路可以不变。从这里可以看出，BSC 其实也是承担了一定的交换功能的。



（2）陆地接口

所谓陆地接口的叫法，是和 Um 口这个空中接口相对应的，它的作用是往前串联 BTS，往后串联 MSC。本接口为相关的物理链路提供正确的格式和阻抗匹配。在我国，一般采用的链路类型是 2.048Mbit/s 的 E1 电路，至于 T1 电路，那是北美标准，我们可以不用去管它。

（3）链路控制

链路控制处理器的主要工作是维护对每个 BTS 的通信以及对 MSC 的通信。另外，它还在 BSS 中进行全面的话务管理，以确保通话传输正确，并可提供给 MS 最佳的小区以实现通信。它包含以下两部分。

① 和 BTS 的通信——GSM 话务处理

BSC 的 GSM 话务处理对第三层话务管理操作负责，包括连接信令（到特定的 MS 称之为连接信令）和无连接信令（如复位、负载限制、阻塞相关的消息）。这些消息是通过无线信令链路（RSL）把 BSC 通话处理连接到 BSS 内 BTS 相关的 GSM 通话过程。连接信令和无连接信令这两个 GSM 话务处理部分共同维护话务的连续。

② MSC 链路处理

MSC 链路处理就是要完成 MSC 和 BSC 之间的通信，所采用的是消息传递链路（MTL）。这个过程处理 MSC 接口所要求的第二层和第三层消息协议。MTL 携带与话务处理和操作状态相关的信息。

（4）同步时钟

如果把总线理解为铁路大动脉，信息理解为在铁路动脉上运动的火车的话，那么这个同步时钟就等同于列车时刻表了。大家的时间必须统一，必须同步，要不麻烦就大了。对于 BSC 来说也是如此，这么多的进程必须配备一个统一的时钟源以确保所有进程同步。

上面的 GSM 话务处理的内容其中一部分是 BSC 独有的工作：陆地链路管理、信道分配、无线信道管理、信道配置管理、切换控制；另一部分则是需要 BSC 和 BTS 配合才能完成的工作：跳频、业务信道管理、控制信道管理、加密、寻呼、功率控制、切换控制。下面就来关注这些工作具体是怎么实现的。

首先，无论是话务信息也好，控制信息也好，对于 GSM 这么一个 TDMA 系统，它们都是以时隙为单位在各种控制或数字处理板件之间进行信息交换的。来自 BTS 的信息也好，来自 MSC 的信息也罢，都必须有一条通路，通过这条通路将信号送到合适的处理单元，才能够完成信息的处理和控制命令的传送。完成这个作用的通道我们称之为“TDM 总线”，也就是时分复用总线，与我们上文所说的数据总线的作用非常类似。这根总线的作用是最关键、最核心的，没有它，一切话务信息和控制信息都无法路由到它想去的地方，那么也就无所谓通信了。

无论是摩托罗拉还是华为的 BSC 系统，这根总线都是必不可少的，不过名称各有不

同，摩托罗拉称之为时分复用（TDM）通路，还把它分为交换机公共通路和出局公共通路两类，甚是麻烦，如果不纠缠于细节的话，我们就当这两根线是一根好了，对于我们理解问题不会有本质的区别。华为就干脆没有为它单独命名，将它和一些板件笼统地称之为 TDM 交换子系统。对于本书而言，我们不需要记忆这些复杂的东西，我们只需要知道有这么一根总线，这根总线的作用就是路由话务和控制信息就行了。

很明显，总线就是总线，就如同公路就是公路一样，它只有一个通道的功能，至于把货物从一条道转运到另一条道以完成物流，把信息从某个端口某个时隙交换到另一个端口另一个时隙，这活它可干不来，得另外找人来干。这不，摩托罗拉招了一个人，叫做 KSW（Kiloport Switch Board，千端口交换板）；华为也招了一个人，叫做 GTNU 板，干的也是同样的活。KSW 的主要工作就是进行时隙交换，用于工作的 TDM 公共通路，以每次呼叫为基础在 BSC 中路由逻辑信道。于是，BSC 的架构在 TDM 总线的基础上增添了一些元素，如图 4.31 所示。



图 4.30　TDM 总线

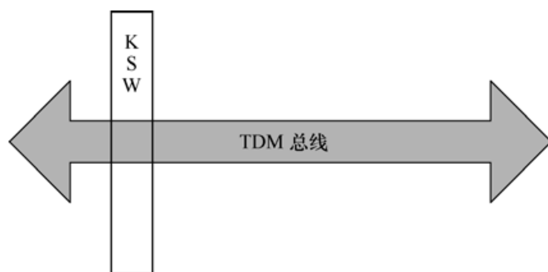


图 4.31　千端口交换板（用于时隙交换）

动态交换工作有人做了，现在我们来关注链路控制工作。至于陆地物理链路，是不用多费心思的，就是一根 2M 线，横竖没有别的东西，易于理解和掌握。

2. BSC 中的链路

第 1 章我们对 RSL（Radio Signalling Link，无线信令链路）、OML（Operations and Maintenance Link，操作和维护链路）、MTL（Message Transition Link，消息传送链路）进行了一番水煮，再加上 CBL（Cell Broadcast Link，小区广播链路）和摩托罗拉特有的 XBL（XCDR Base Link，变码器基站链路），链路不可谓不多，下面我们就对它们逐一作一番介绍。这一部分是 BSC 中最复杂的部分，希望大家要有耐心。

（1）消息传递链路（MTL）

其中，MTL 存在于 MSC 与 BSC 之间，采用 C7 信令系统，此链路在 BSC-MSC、MSC-MS 之间提供所有控制信息，包括：初始连接请求、通话过程中任何属性的变化、处理切换。



（2）无线信令链路（RSL）

RSL 存在于 BSC 和 BTS 之间。RSL 使用格式化的 LAPD 信令，一般都需要占用一个 64kbit/s 的时隙，也有占用一个 16kbit/s 的信道的。该链路主要是为 BTS 上的话务处理软件提供支持，允许 BSC 向 BTS 发送和接收控制信息。它也支持统计信息的收集和故障报告工作。

具体一点说来，RSL 的主要作用有以下两点：

① 实现 MS 与 BSC 的业务管理消息的互通；

② 在 BSC 的控制下完成一部分无线资源管理功能。

对于 MS 与 BSC 之间的业务管理消息，从处理的角度划分又分为两种：

① 透明消息，即不需要 BTS 解释或处理而直接转发的消息；

② 非透明消息，包括只在 BSC 和 BTS 之间传递的消息和 BTS 必须处理或是由 BTS 构造的消息。

业务管理消息从功能的角度来划分又可以分为以下 4 组。

① 无线链路管理消息。用于管理无线路径上的数据链路层，包含链路的请求、建立、释放；确认证实方式和非确认证实方式下透明 Um 接口第三层消息的转发。

② 专用信道管理。用于专用信道（SDCCH 和 TCH）的管理，包含专用信道的激活、信道模式的改变、加密和功率控制等。

③ 公共信道管理。用于公共控制信道（CCCH）的管理，包含随机接入的链路请求、立即指配、寻呼消息和短消息的小区广播。

④ 载频的管理消息。用于载频信息的管理，包括 SACCH 的系统消息管理、流量控制、错误报告、无线资源指示。

说起来这部分内容是非常复杂的，尤其是当我们对信道以及信令流程还并不熟悉的时候，要理解这部分内容尤其显得困难。这并没有关系，我们现在所需要做的就是对上述内容有一个概念和一个整体的认识，细节可以留待后面去学习。本章并不打算就这一内容进行展开叙述。

（3）操作与维护链路（OML）

本链路用于 BSS 和 OMC 之间的控制和通信，OML 使用 X.25 协议。OMC 使用 OML 用来完成以下工作：

① 加载软件；

② 加载配置参数；

③ 发送消息到 BSS，并从那里接收消息；

④ 从 BSS 收集统计信息；

⑤ 故障/事件管理。

（4）小区广播链路（CBL）

本链路存在于 BSC 和小区广播中心（CBC）之间。CBL 使用 LAPB/X.25 协议。本链路用来把来自外部 GSM 网络的短消息服务（SMS）小区广播信息传递到 BSC。

（5）变码器基站链路（XBL）

这是摩托罗拉所独有的链路，摩托罗拉有一个自己独有的设备称之为 XCDR，这个设备的功能是将 Abis 接口的 16kbit/s 的信道进行复用，组合成适合在 A 接口传输的 64kbit/s 的 PCM 链路。其作用就是进行“16kbit/s—64kbit/s”的链路转换，也就是 GSM 规范中所说的 TRAU 功能。对于华为和诺基亚西门子而言，都是采用板件来完成该项功能的，华为的称之为变码器（TCSM），诺基亚西门子的称之为 TURE。

说到这里，作者想把第 1 章关于这些链路的图示放在此处供大家浏览一下，以便对这些链路在各组成部分的位置有个整体的概念。

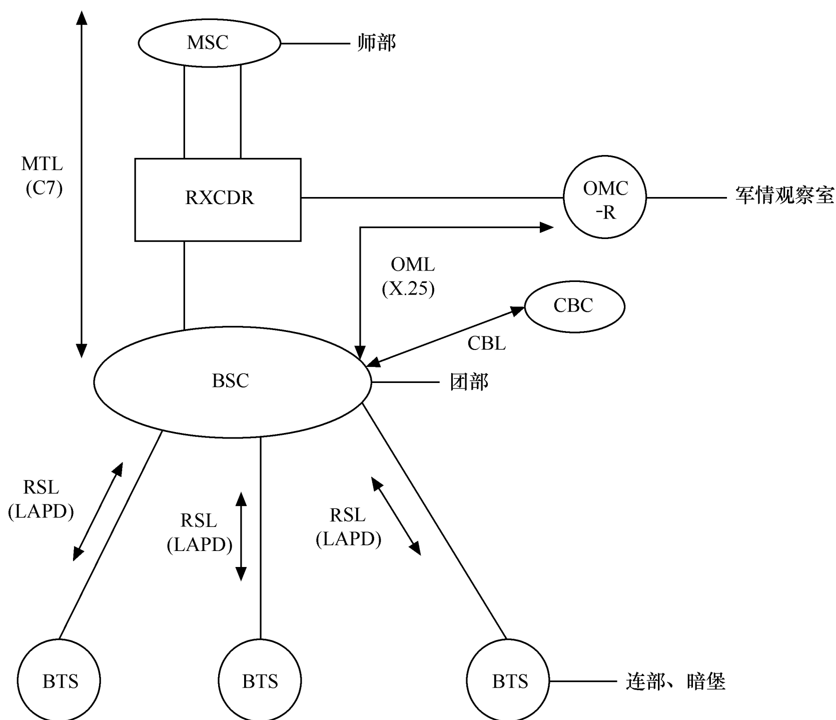


图 4.32　信令链路

这么多信令链路都是要有人处理的，谁来处理呢？在摩托罗拉的构架中，安排了一个叫做 GPROC 板（Generic Processor Board，通用处理板）的伙计来干这活，华为则不一样，它把这些工作分配到了 3 块板件上，分别称为 GXPUM 板（寻呼控制、系统消息管理、信道分配、基站公共业务管理、语音呼叫控制、分组业务控制、切换控制、功率



控制)、GXPUC 板（短消息（CBC）的接口、CBCH 调度广播消息）以及 GSCU 单板（为所在插框提供维护管理和交换平台)。华为架构与摩托罗拉的架构没有本质的区别，区别是摩托罗拉是一块单板完成这些工作，而华为则按照自己的意图对工作进行了分解。

无论是摩托罗拉的 GPROC 板还是华为的 GXPUM 板，其在整个系统架构中的地位都是很重要的，相当于 CPU 在计算机中的地位。GPROC 板与 CPU 也有相似之处，GPROC 板是采取分布式控制的，相当于一个多核处理器。一个 BSC 中可以有多块 GPROC 板，分别处理不同的链路，GPROC 板之间有专用的总线通信在 GPROC 板之间进行仲裁，保证数据总线上某个时刻只有一块 GPROC 板在操作。GPROC 板与多核 CPU 的区别之处在于，GPROC 板要处理的链路是相对固定的，你分配好哪块 GPROC 板处理哪条链路之后，它就一直这么操作下去，直到你下次改变配置为止。你不妨把一个 BSC 中的多块 GPROC 板看成一个可扩容的专用多核处理器，你再多插一块 GPROC 板就相当于三核变四核，四核变五核了。而基于 Intel 架构或 AMD 架构的这种多核处理器则称为通用多核处理器，它要干的活不止处理几条链路这么简单，所谓通用就是什么都得干。另外，不同的核之间分配的工作也不像 GPROC 板这种是固定的，还需要事先配置。

我们把 GPROC 板添加进去，那么 BSC 的构架就变成了图 4.33 所示的样子。



图 4.33　增加了 GPROC 板的 BSC 架构

现在我们有了 TDM 总线，有了时隙交换器件，有了 CPU（GPROC）板，可以说，BSC 最重要的工作已经完成了。当然，要让它成为一个商业系统，走到这里还远远不够，我们还需要对我们的系统完善，再完善。

首先，我们既然把 GPROC 板比作了多核处理器，那么多核处理器首先面临的一个问题就是怎样处理使用总线的问题。大家都是 CPU，大家都要调度总线，这就不可避免地会有冲突，有冲突就要有仲裁。这种仲裁机制在计算机网络中并不鲜见，一种在局域网中很常见，称为“CSMA/CD”具有碰撞检测的载波侦听多路访问机制，其工作原理就是大家都侦听信道上的载波，一旦发现空闲了就把自己的信号发送出去，如果遇到碰撞，那就延迟一个随机的时间再发送出去；另一种称之为令牌环（Token Ring）机制，一个大圆圈，令牌逐次传递下去，拿到了令牌的终端可以发送信息，没有拿到令牌的人继续等待，你可以把它理解为 KTV 唱歌，令牌就是麦克风，麦克风逐次传递，拿到了麦克风的可以

唱歌，没拿到的等着人家传过来。GPROC 板采取的就是令牌环机制，GPROC 板之间用 LAN 总线连起来形成令牌环，另外，LAN 总线还可用于 GPROC 板之间互相传递数据。为了建立 LAN 总线，需要添加一块 LANX 板，我们对图 4.33 略作修改，就形成了图 4.34。

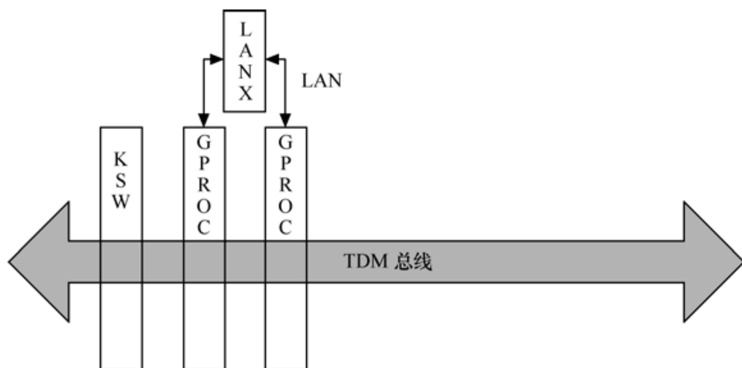


图 4.34　GPROC 板的通信

上面还缺些什么呢？想都不要想，连个时间板都没有，就好比铁路上没有列车时刻表，那还混啥子呢，赶紧加上。这就是 GCLK 板（Generic Clock Board，通用时钟板），在华为系统中，也有时钟板，称为 GGCU 板。

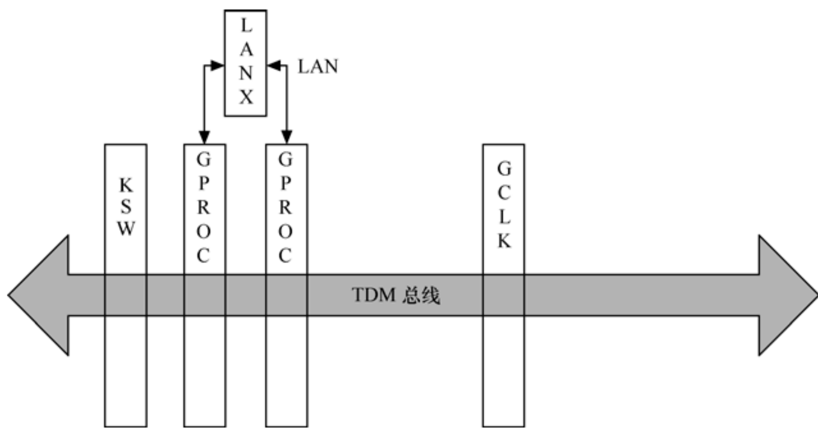


图 4.35　GCLK 时钟板

我们在 3.2.1 节中说过，GSM 通过语音编码之后就产生了 13kbit/s 的源码速率，通过信道编码在空中接口发送时的速率为 22.8kbit/s。BTS 对信道解码后又恢复了 13kbit/s 的语音编码速率，然而为了形成速率为 16kbit/s 的 TRAU 帧以便于在 Abis 接口和 Ater 接口传送，我们还需要添加速率为 3kbit/s 的信令。然而，到了 A 接口就是 64kbit/s 的速率传输了，这样做是有历史原因的，因为 PSTN 就是这么做的，那么就需要一个变码器来进行转换，这个码速转换器在摩托罗拉里是独有的，称为 Transcode，其核心其实也是一块



板子，叫做 XCDR。这与华为的 TCSM 板、诺基亚西门子的 TURE 板其实也很相似。

我们把 XCDR 添加上去，就得到了图 4.36。

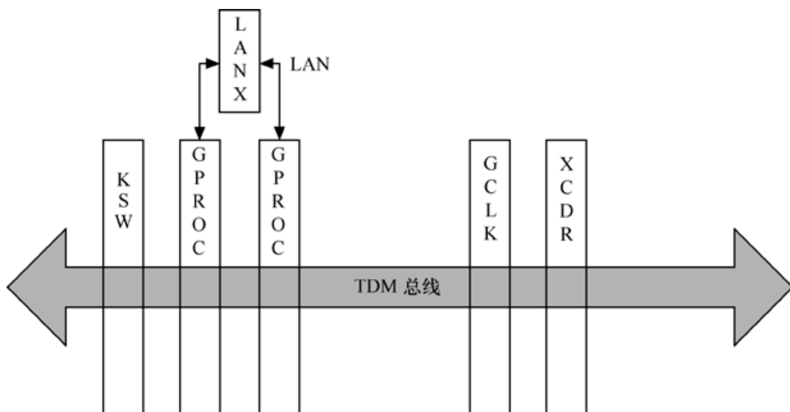


图 4.36　XCDR 码速变换

到这里，还差一个功能，Abis 接口也好，A 接口也罢，使用的都是 2M 线，2M 线是一个串行的导线，而总线就不一样了，总线是多根导线并行在一起的，那么在接口的地方就必须进行串/并转换。在摩托罗拉构架中，这个功能是由一个叫做 MSI（Mutiple Serial Interface）的功能板来完成的，如图 4.37 所示。对于华为构架而言，那就太复杂了，华为共有 8 块板子来完成这个功能，其中 4 块板子采用 E1 传输，4 块板子采用 STM-1 传输，分别对应 A 接口、Abis 接口、Pb 接口和 Ater 接口。

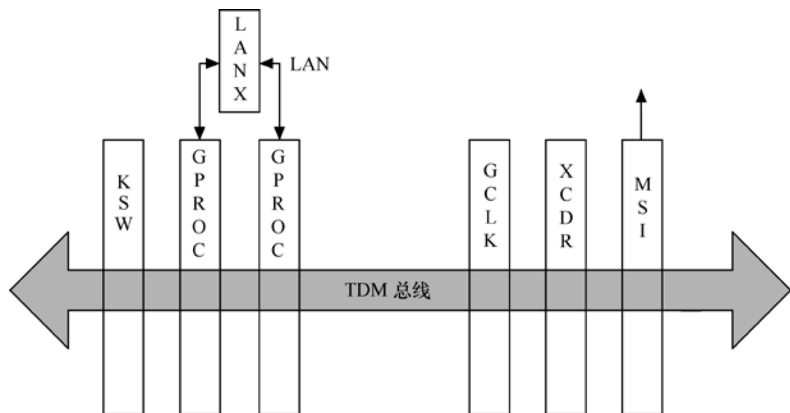


图 4.37　MSI 板

到这里，基本大功告成了，不过各位想想，又是 KSW，又是 GCLK，又是 MSI 板，干活的这么多，谁来对它们的工作进行监控和管理呢？按常理，当然应该是 GPROC 板。不过总得有条通道啊，TDM 总线是用于语音和信令通道的，占用这个可不太妥，不如再搞一条专用总线吧，这就是 MCAP（Motorola Cell Advance Processor，摩托罗拉单元高

级处理器）总线，用于连接 GPROC 板和其他板子。

在华为架构中，也有类似的处理方式，华为称之为 GE 交换子系统，用于控制其他板件的通信。添加了 MACP 总线的架构如图 4.38 所示。

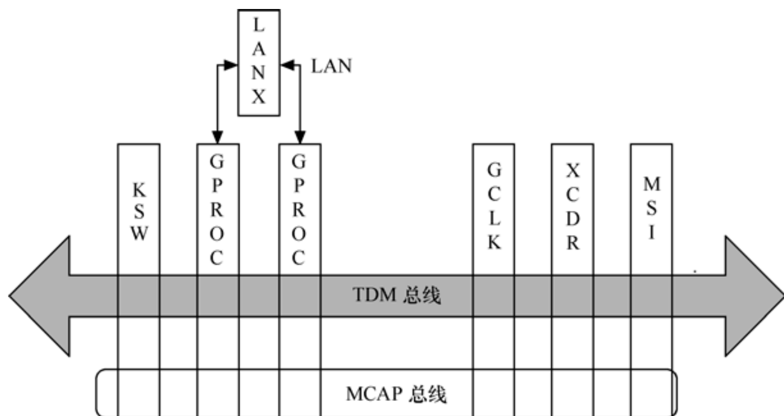


图 4.38　基本完整的 BSC 结构图

到这里，还只能称之为基本完整，有很多琐碎的环节尚未考虑，比如说总线的扩展、机柜的扩展、环境的监控、供电系统等。应当说那些并不是通信的核心环节，出于篇幅以及内容方面的考虑，我们把那些内容给省略了。

4.7　交换子系统——MSC、VLR与HLR

本书侧重的是无线通信，也就是 BSS 侧，前面两节已经对基站收发信机（BTS）和基站控制器（BSC）作了非常详尽的介绍。对于交换的内容，我们需要了解，但不必太深入。因此，本书将 NSS 交换子系统放到一节里加以阐述。

4.7.1　移动交换中心（MSC）

1. 交换机的诞生

鲁迅先生说：世界上本没有路，走的人多了，也便成了路。这句话也可以套用在 MSC 上，世界上本来是没有交换机的，打电话的人多了，也就有了交换机。想当年贝尔发明电话的时候，就是一根线从这头牵到那头，可没有考虑过需要什么交换机。后来用户多了，这种直接牵线的方式就行不通了，如图 4.39 所示。



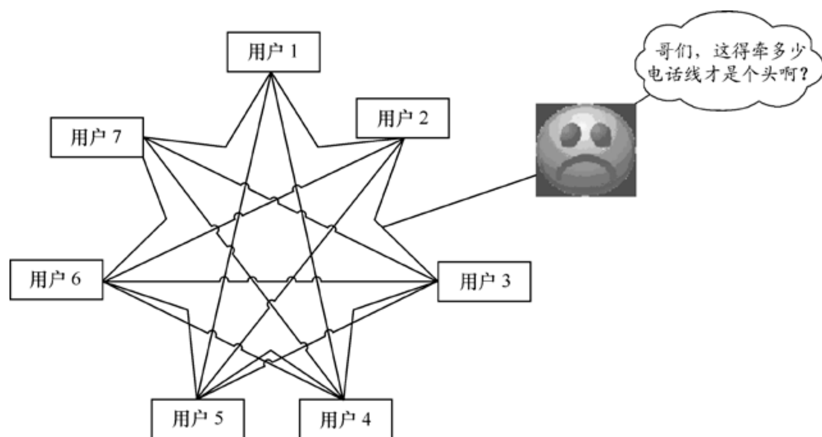


图 4.39　装线工的烦恼

于是交换机应运而生，最早的交换机是人工的。如果放的电视剧是以 20 世纪 30、40 年代为背景的话，大家还经常可以看到这样的场景。某人摇几下电话的转轴，提起电话，接电话的却不是要找的人，而是接线员，然后对接线员说："给我接×××"，接线员随后接到相应的人。这打电话找人可够麻烦的。

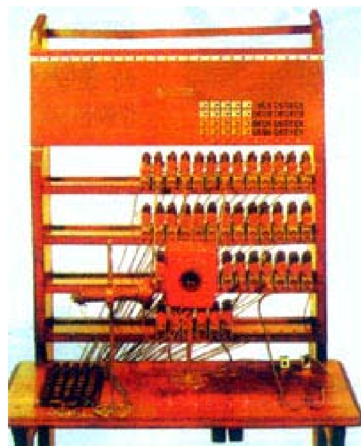


图 4.40　早期的人工电话交换机
（能为 50 家电话用户提供服务）

2. 程控交换机

麻烦就麻烦，大家也就忍了。有电话总比什么"飞鸽传书"、"八百里加急"要强多了吧，不就是不能直接连通还需要话务员转接一下电话吗，这有什么了不得的。可是发明往往就源于不能忍，爱迪生不能忍受煤油灯那微弱的光亮，于是发明了电灯；瓦特不能忍受马车的速度与低效，于是发明了蒸汽机车。现代程控交换机发明的最初动机，也源于不能忍。

最早的自动电话交换机是在 1892 年 11 月 3 日投入使用的。那是美国人史端乔创造的步进制自动电话交换机。史端乔是美国堪萨斯城的一个殡仪馆老板，他发觉每当城里发现死亡事件时，用户往往向话务员（人工交换机）说明要接通某一家"殡仪馆"，而那位话务员总是把电话接通到另一家殡仪馆。这使史端乔很生气，发誓要将电话交换机自动化。结果他成功了，取得了第一个自动电话交换机的专利权。以后这种交换机就称为史端乔交换机。对通信作出巨大贡献的莫尔斯、贝尔、史端乔居然都非科班出身，不得不感叹有梦想对于一个人而言有多么的重要！

史端乔发明的是步进制交换机，这种"步进制"自动交换机的特点是由用户话机的

拨号脉冲直接控制交换机的接线器动作。后来又陆续出现了"旋转制"、"升降制"和"纵横制"的交换机。这些交换机都有一个共同特点，那就是机械式的，直到微处理器和半导体存储器大量问世之后，才引发了交换机电子化的革命，我们将这种交换机称为"程控交换机"。程控交换机的典型结构如图 4.41 所示。

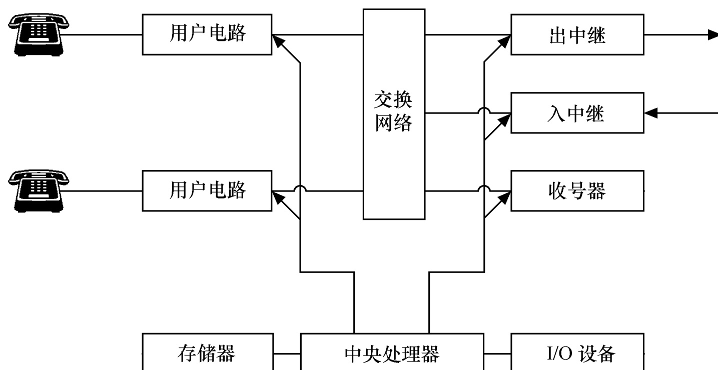


图 4.41　程控交换机结构框图

3. 交换机的原理

我们再来说说交换机。交换机究竟要交换什么呢？交换机的交换功能有两项，一是母线交换，也就是信号从这根线换到那根线；二是时隙交换，也就是从这个时隙交换到另一个时隙。

图 4.42 所示就是将占用母线 1 时隙 5（TS5）的语音信号经过数字交换网络以后换到了母线 2 时隙 18（TS18），由另一个用户接收。

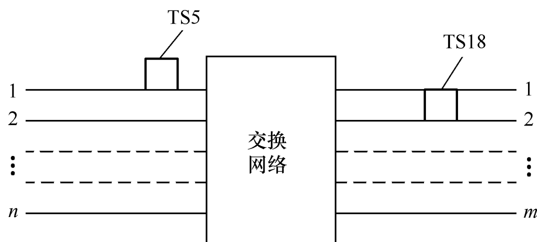


图 4.42　数字交换网络进行时隙交换

我们通常用两种数字接线器来完成交换工作：时间（T）接线器和空间（S）接线器。它们的基本分工是：空间接线器负责实现母线交换，时间接线器负责实现时隙交换。

4. 空间（S）接线器

空间接线器相对而言工作原理比较简单，就是一个交叉的电子矩阵，共有 n 个入端和 n 个出端，形成 $n \times n$ 矩阵，由 n 个控制存储器控制。每一个控制存储器控制同号输出端的所有交叉点，这叫做"输出控制"。控制存储器的工作方式称为"控制写入，顺序读出"。空间接线器究竟是如何工作的呢，下面我们详细分析。

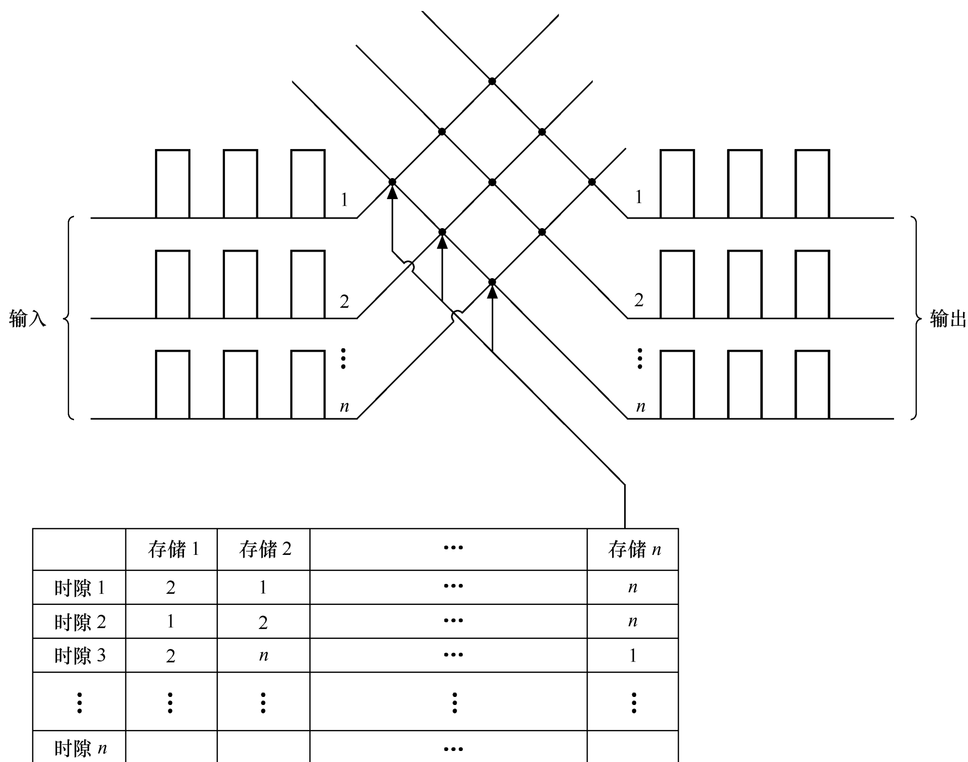
空间接线器的作用就是完成信号在空间上的交换。在空间接线器的左边有 N 条线，它们来自不同的地方。在空间接线器的右边也有 N 条线，它们去往不同的地方。现在左



边的 1 号线上走的信号，它们分别要去往右边的 2 号线、1 号线、6 号线、7 号线……，这该咋办？这就轮到空间接线器大显神威了，它通过交叉矩阵把信号送到不同的线上去。

我们可以把空间接线器左右两边一条条的线看作铁路，那么空间接线器就是铁路的枢纽——火车站。火车站的一项重要工作就是将来自火车站左边某条铁路的火车通过铁路扳道工的工作将它送到右边能通向它目的的那条铁轨上去。

这样一来，图 4.43 的那张表也就可以理解为火车调度员下发给扳道工的指令了。我们来看看这些指令都怎么理解。最左边一列标的是时隙，相当于列车时刻表。扳道工嘛，2:00 和 2:30 要干的工作肯定是不一样的，2:00 的时候 1 号进线还要和 2 号出线相连，到 2:30 的时候来的就是下一趟车，下一趟车和这趟车的目的地不一样，说不定 1 号进线就得连 1 号出线了。最上面一列标的是存储单元，每个存储单元控制对应的输出端的所有交叉点。读懂了控制存储器的原理，我们下面就对控制存储器的内容进行详细的解释。



	存储 1	存储 2	…	存储 n
时隙 1	2	1	…	n
时隙 2	1	2	…	n
时隙 3	2	n	…	1
⋮	⋮	⋮	⋮	⋮
时隙 n			…	

图 4.43　S 接线器示意图

（1）1 号控制存储器的 1 号单元内容为“2”，表示 2 号入端和 1 号出端接通。

（2）2 号控制存储器的 1 号单元内容为“1”，表示 1 号入端和 2 号出端接通。

……



（n）n 号控制存储器的 1 号单元内容为“n”，表示 n 号入端和 n 号出端接通。

在时隙 2 的时候，可以根据上面的论述推出相应的结果。可以看到，空间接线器是不改变时隙号的，它是按时隙读取数据的，所以无法完成时隙的交换。空间既然交换了，那么时隙又该如何交换呢？

5. 时间（T）接线器

进行时隙交换采用的是 T 接线器，T 接线器的结构如图 4.44 所示。图 4.44 所示的是“输出控制”方式的 T 接线器，由话音存储器和控制存储器两部分组成。

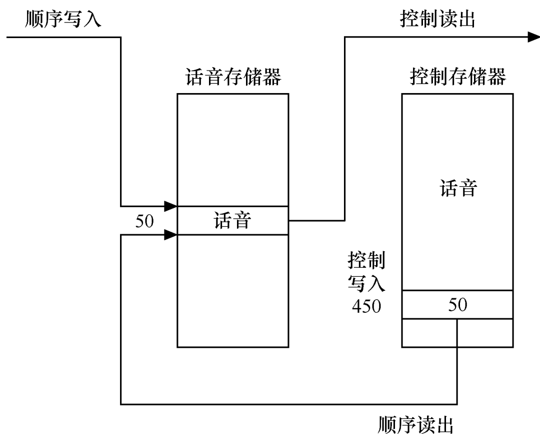


图 4.44　输出控制的 T 接线器

现在我们就来看看该如何完成时隙交换。假设语音信号在 50 号时隙上，要把它交换到 450 号时隙上去，该怎么办呢？

我们可以通过 CPU 和控制存储器来完成这项工作。CPU 通过软件在控制存储器的 450 号单元写入“50”。这个写入是由 CPU 来完成的，所以称之为控制写入。

控制存储器的读出是按顺序来的，称之为顺序读出。它由定时脉冲控制，按照时隙号读出相对应的单元内容。如 0 号时隙就读出 0 号时隙单元的内容，1 号时隙就读出 1 号时隙单元的内容，依此类推。

也就是说，控制存储器是“控制写入，顺序读出”的。而话音存储器的工作方式则恰好相反，是“顺序写入，控制读出”的，也就是说，写入的时候是按照单元顺序一个一个来的，而读出不是。

话音存储器在定时脉冲的控制下，按顺序将不同时隙的话音信号写入到相应的单元中去。写入的单元号和时隙号一一对应。而读出时则要根据控制存储器的控制信息（读出数据）来进行。由于话音存储器的输入话音信号不受 CPU 控制，而输出话音信号受到 CPU 控制的控制存储器的控制，因此把它称为“输出控制”方式。

现在来对图 4.44 做具体一点的说明。在语音存储器这一侧，话音的输入时隙号为 50，在定时脉冲控制下就可写入到 50 号单元中。

而 CPU 在控制存储器中的 450 号单元写入的内容为“50”。在定时脉冲的控制下，在 450 号时隙的时间里，从控制存储器的地址单元 450 中读出内容为 50，把它作为语音存储器读出地址，立即读出语音存储器的 50 号单元，这正好是原来在 50 号时隙写入的话音信号内容。此时话音信号 50 号单元的信息终于被放出来了，但是时间已经拨到了



450 号时隙，这样就把语音信号从 50 号时隙交换到了 450 号时隙，从而实现了时隙交换。

6. T-S-T 三级网络

在大型程控交换机中，数字交换网络的容量比较大，只靠 T 接线器或 S 接线器是不能实现的。必须将它们结合起来，才能达到要求，下面我们就举一个 T-S-T 三级网络的例子，如图 4.45 所示。

图 4.45　T-S-T 三级网络示例

实际的网络可能比 T-S-T 三级结构更复杂，日本 NEC 公司生产的 NEAX-61 是典型的 T-S-S-T 时分交换网络结构，而意大利 Telettra 公司的 DTN-1 数字交换机所采用的结构是 S-S-T-S-S 交换网络，这种网络是在两侧各配备两级 S 型接线器，中间为一级 T 型接线器。



对于 T-S-T 网络以及更复杂的网络，这里就不再展开叙述了，否则本书就变成《现代交换技术》了，感兴趣的朋友可以阅读相关的资料。

7. MSC

上面我们花了不少篇幅来描述一个交换机是怎样完成交换功能的，从母线的交换到时隙的交换都有了一个清晰的概念。不过对于移动交换中心（MSC）来说，光有交换功能是不够的。

MSC 处于 NSS 交换子系统的核心位置（如图 4.46 所示），要完成的工作自然也就很多。

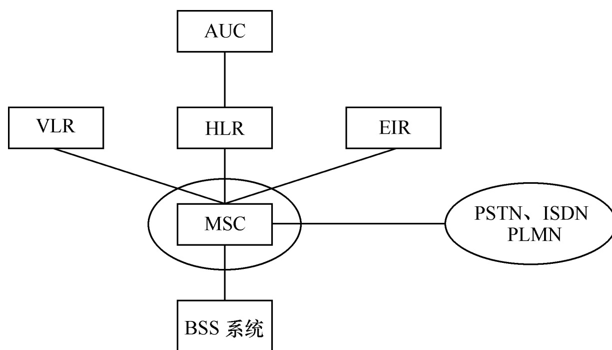


图 4.46　MSC 处于 NSS 与 BSS 以及其他网络连接的关键位置

MSC 的主要工作有：

（1）完成话音的接续功能，主要工作就是我们前面所说的交换，包括被叫用户所在地查询与寻呼、信道的分配、话务量控制以及计费等功能；

（2）作为网络的核心，配合 HLR/AUC 和 VLR 完成移动用户位置登记、自动漫游、合法性检验等功能；

（3）配合 BSC 完成跨 BSC 的切换，以及通过信令来指示无线信道的建立和释放；

（4）提供面向系统其他功能实体和面向固定网（PSTN、ISDN 等）的接口功能。

BSC 处理用户呼叫所需的数据与以下 3 个数据库有关，分别是 HLR、VLR 和 AUC，用户当前的位置和状态信息对于 MSC 来说非常重要。下面就对这 3 个数据库逐一进行介绍。

4.7.2　GSM 中的根 DNS——归属位置寄存器（HLR）

在 GSM 系统中，虽然用户可以在整个 GSM 网络中漫游（国际漫游需在签约运营商的网络中漫游），但是移动用户只需要向一个国家的一个运营者进行登记、签约和付费。这个运营者就是用户的归属局，归属局存放了所有用户的签约信息的寄存器就称为归属位置寄存器（HLR，Home Location Register）。

HLR 中的数据通常包含两类：第一类是静态数据，也称为用户参数，包括用户号码（MSISDN）、移动用户识别码 IMSI 号、Ki 号、接入的优先等级、补充业务等；第二类是动



态数据，也称为用户的位置信息，用户会经常漫游到 HLR 所服务的区域之外，那么 HLR 需要登记由该区传来的位置信息。这样做的目的是保证当呼叫任何一个不知道当前所在哪一个地区的移动用户时，均可以由该移动用户的 HLR 获知它当前所处的地区，进而建立连接。

4.7.3　GSM 中的本地 DNS——访问位置寄存器（VLR）

某种意义上，你可以把 HLR 理解为一个 DNS，因为它也有寻址的功能。我们知道，DNS 是一个分布式的数据库，而且是分级的。DNS 的整体构架由根 DNS 服务器、顶级域名 TLD 服务器和权威 DNS 服务器组成，如图 4.47 所示。

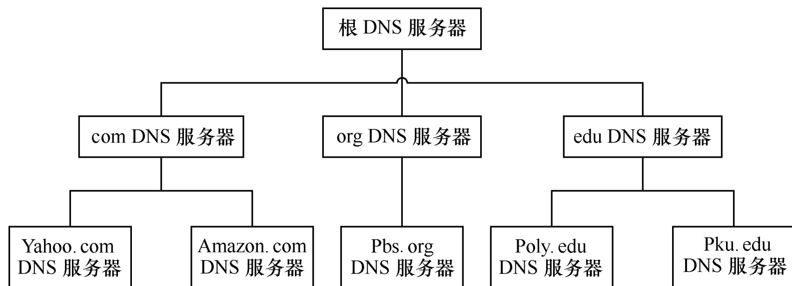


图 4.47　DNS 构架图

DNS 需要你从根 DNS 服务器一级一级地向下寻址，当然，你或者你的本地 DNS 有本地缓存除外。HLR 和 VLR 与此也有点类似，不过是一个两级结构。HLR 可以指向 MS 所在的 VLR，VLR 再指向 MS 所在的位置区，最后通过位置区寻呼找到该用户。

VLR 往往和 MSC 合并在一个设备实体中，因为每一次呼叫，这两者之间总有大量的信令流通。如果分放在两个实体设备中，那么会使它们之间的信令链路承受高负荷。

VLR 是用来存储用户当前位置信息的数据库。当用户漫游到新的 MSC 控制区时，它必须向该地区的 VLR 申请登记。VLR 要从该用户的 HLR 查询有关的参数，要为该用户分配一个新的漫游号码（MSRN），并通知其 HLR 修改该用户的位置信息，准备为其他用户呼叫此移动用户时提供路由信息。如果移动用户从一个 VLR 服务区移动到另一个 VLR 服务区，HLR 在修改了该用户的位置信息后，还得通知原来的 VLR 删除此移动用户的位置信息。

VLR 是一个动态的数据库，它的数据随用户的变化而不断改变；VLR 也相当于一个分布式的 HLR。它也存储了两类信息：一是当前 VLR 下的用户参数，该参数是从 HLR 中获得的；二是当前交换区 MS 的位置区标识（LAI）。

4.7.4　GSM 系统的守护神——鉴权中心（AuC）

AuC 属于 HLR 的一个功能单元部分，专用于 GSM 系统的安全性管理。它的作用是产生一个三参数组——RAND、SRES 和 Kc 的功能实体。这几个参数用于确定移动用户

的身份和对呼叫进行加密。

AuC 存储着鉴权信息，用来对用户进行鉴权，防止非法用户的接入；AuC 还存储着密钥，用来对无线接口上的语音、数据、信令信号进行加密，保证用户的通信安全。

每个用户在运营商处进行开户登记的时候，就会被分配一个用户号码（MSISDN 号）和用户识别码（IMSI 号）。IMSI 通过 SIM 卡写卡机写入 SIM 卡中，同时在写卡机中又产生了一个对应此 IMSI 的唯一的用户密钥 Ki。IMSI 号与 Ki 号在 SIM 卡和 AuC 中都有存储，便于核对。

AuC 的两大功能是鉴权和加密，AuC 中有一个伪随机码发生器，用于产生一个不可预测的伪随机数（RAND）。RAND 和 Ki 经 A8 算法（加密算法）产生一个 Kc，经 A3 算法（鉴权算法）产生一个响应数（SRES）。由 RAND、SRES、Kc 一起组成了一个用户的三参数组，AUC 每次对一个用户产生 7～10 组三参数组，传送给 HLR，HLR 将其存储在该用户的用户资料库中。

VLR 一次向 HLR 要 5 组三参数组，每鉴权一次用 1 组，当只剩下 2 组时，再向 HLR 要 5 组，如此反复。RAND、SRES、Kc 这三参数组都有什么作用呢？

1. 鉴权

鉴权的目的就是为了防止非法用户使用网络。当用户通过 RACH 信道请求接入网络时，MSC/VLR 通过控制信道将 RAND 传送给用户。SIM 卡收到 RAND 之后，用 RAND 和 SIM 卡中的 Ki 经过 A3 算法得到应答数 SRES，然后将其传送给 MSC/VLR。MSC/VLR 将收到的 SRES 与三参数组中的 SRES 进行比较，如果相同就允许接入，若不同则拒绝，如图 4.48 所示。

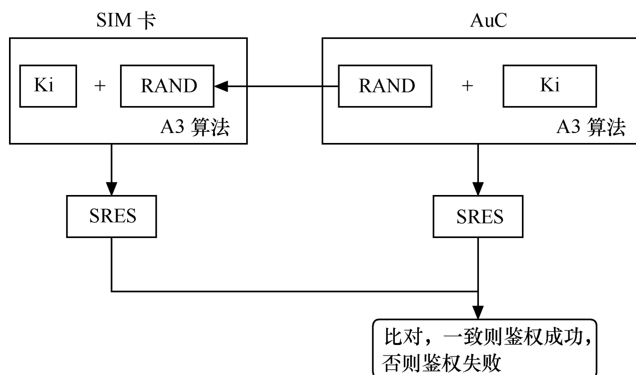


图 4.48　鉴权过程

2. 加密

我们知道，空中接口的电磁波是向四面八方传播的，拦截是很容易的，为了让用户的信息不被窃取，用户的对话不被窃听，我们有必要对在空中接口传送的数据进行加密。



MS 侧通过 A8 算法就得到 Kc，根据 MSC/VLR 发送的指令，BTS 和 MS 侧同时使用 Kc。在 MS 侧，由 Kc、TDMA 帧号以及用户数据一起经过 A5 算法，对用户信息数据流进行加密，俗称扰码，扰码之后在无线路径上传递。

在 BTS 侧，把收到的数据流与 TDMA 帧号、Kc 一起再经 A5 算法解密后传递给 BSC 和 MSC。加密算法如图 4.49 所示。

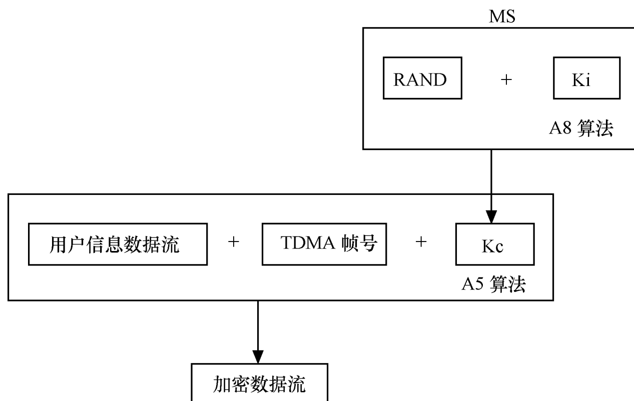


图 4.49　加密算法

4.8 这是你的门牌号码——GSM编号计划

管理一个庞大的系统需要科学的方法，而对这个系统中的每一个元素都进行编号管理就是方法之一。邮政系统无疑是一个庞大而复杂的系统，但是邮政局却有能力把你的信件送往中国任何一个角落中的任何一个人。这种能力一方面源自交通和物流的大发展，另一方面也有赖于邮政体系对于地理层面的良好的编码计划。

俺们前面唧唧呱呱地讲编码计划，搞得神神秘秘的，其实在邮政局的信封上体现得很简单，就是“收信人地址+收信人”，这两条就标识了一个唯一的收信对象，保证邮局不会送错。

一个好的编码计划需要有两点，一是标识的唯一性，比如说下面的收信地址“湖南省长沙市沿江大道×××号”，如果长沙不止一条沿江大道，那就尴尬了，邮递员面对两个地点将会无所适从；二是标识要方便检索，比如你要对地理位置进行一套编号，你完全也可以按经纬度进行编码，这种编号方式也绝对是唯一的，“东经 112.56，北纬 28.37”，呃，你打算让邮递员带一个 GPS 出门么？对于信件的查找和分类而言，这显然没有“省+市+县（区）+街道+门牌号”这样的分级检索方式好用。

对于 GSM 的编号计划而言，也需要满足以上两个条件。首先，唯一性是必须满足



的，要是你的手机号与别人的相同，或者某个信令点的编码和另一个信令点的编码相同，不用说大家也知道会发生什么事；方便检索肯定也是要的，大家都知道有个叫“手机归属地查询”的软件，其诀窍就是这个软件有一个数据库，数据库根据手机号码的第 4～7 位来判定手机的归属地，比如说 133-0731-0000，一看中间的 0731，就知道是来自长沙的。这种编号方式很重要，极大地方便了 HLR 的寻址。

闲话少说，下面我们就来介绍 GSM 系统的编号计划。

GSM 网络是很复杂的，包括交换系统和基站系统。交换子系统包括 HLR、MSC、VLR、AUC 和 EIR 等设备，还与基站子系统、其他网络，如 PSTN、ISDN、数据网、PLMN 之间拥有接口。为了将一个呼叫接至某个移动用户，需要调用相应的实体。因此要正确寻址，编号计划就非常重要。

1. 移动台的国际 ISDN 号码（MSISDN）

MSISDN（Mobile Station International ISDN Number）是指主叫用户为呼叫数字公用陆地蜂窝移动通信网中的用户所需拨的号码。简单一点说，就是你打电话的时候拨打手机号，这个号码采取“E.164”编码计划，号码的结构如图 4.50 所示。

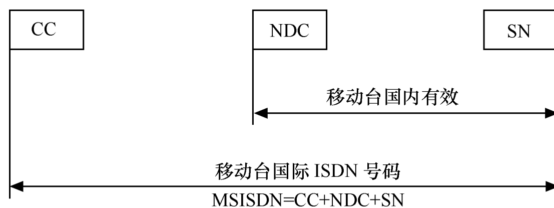


图 4.50　MSISDN 的组成

图中各部分解释如下。

CC（Country Code）＝国家码，即在国际长途电话通信网中要使用的标识号，中国为 86，虽然很多人并不打国际电话，但是对于这个号码应该并不陌生，发短信的时候经常看见一条来自“86139********”的短信，虽然你是给国内的手机用户发短信，但是运营商还是把这个国家码给你加上了。

NDC（National Destionation Code）＝国内目的地码，即网络接入号，也就是平时手机拨号的前 3 位。中国移动 GSM 网的接入号为“134～139”、“150～152”、“157～159”，中国联通 GSM 网的接入号为“130～132”、“155～156”。

SN（Subcriber Number）＝用户号码，采用等长 8 位编号计划。

MSISDN 的前面部分 CC+NDC+H0H1H2H3 其实就是用户所属 HLR 的 GT 地址，这样在入口移动交换中心（GMSC）查询 HLR 时可直接利用 MSISDN 进行信令连接与控制部分（SCCP）的寻址。



如一个 GSM 联通手机号码为 8613007370000，86 是国家码（CC）；130 是 NDC，用于识别网络接入号；07370000 是用户号码的 SN，0737 用于识别归属区。

2. 国际移动用户识别码（IMSI，International Mobile Subscriber Identity）

值得说明的一点是，虽然作为用户的我们平时都是用的 MSISDN 号，但对于通信设备识别用户而言，它们有自己的套路，它们并不用 MSISDN 号，而是使用自己的一套编号计划，叫做“E.212”编号计划。

为了在无线路径和整个 GSM 移动通信网上正确地识别某个移动用户，就必须为移动用户分配一个特定的识别码。这个识别码称为国际移动用户识别码（IMSI），用于 GSM 移动通信网的所有信令中，存储在用户识别模块（SIM）、HLR、VLR 中。

MSISDN 与 IMSI 的关系有点类似于一个人的姓名与身份证号的关系，虽然我们平时都是以姓名相称呼，但是公安局也好、民政局也罢，还是通过你的身份证号来唯一地识别你。甚至你的姓名还可以去修改，但是身份证号却不会变；同样，你也可以去运营商处修改你的号码，只要你的 SIM 卡没扔，你的 IMSI 号还是不会变。

IMSI 号码结构为：

IMSI=MCC+MNC+MSIN

MCC（Mobile Country Code）＝移动国家号码，由 3 位数字组成，唯一地识别移动用户所属的国家，我国为 460。

MNC（Mobile Network Code）＝移动网号，由 2 位数字组成，用于识别移动用户所归属的移动网。中国移动的 GSM PLMN 网为 00，中国联通的 GSM PLMN 网为 01。

MSIN（Mobile Station Identity Number）＝移动用户识别码，采用等长 10 位数字构成，用于唯一地识别国内 GSM 移动通信网中的移动用户。

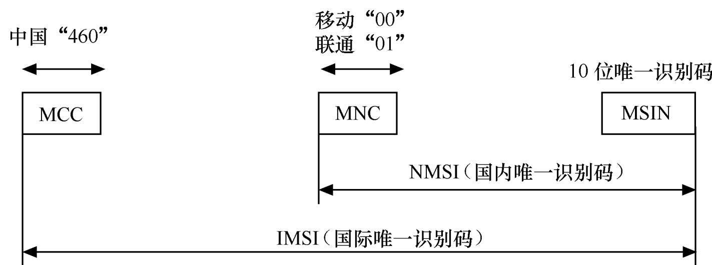


图 4.51　IMSI 号的组成

3. 移动台漫游号码（MSRN，Mobile Station Roaming Number）

MSRN 的结构和 MSISDN 的完全一致，所不同的地方是这个号码是由用户漫游地的 MSC/VLR 临时分配的，不像 MSISDN 是在 HLR 中长久记录的。MSISDN 的作用，是指

向其所在的 HLR，要实现通话，光建立 MSC 和 HLR 的连接是不够的，得建立一个 MSC 和另一个 MSC 的连接，那么由谁来标识用户目前所在的 MSC 呢？都不知道你在哪个 MSC 下自然无法建立连接啊！这就是 MSRN 的功效了。

被叫用户所归属的 HLR 知道该用户目前是处于哪一个 MSC/VLR 业务区，为了提供给入口 MSC/VLR（GMSC）一个用于选路的临时号码，HLR 请求被叫所在业务区的 MSC/VLR 为该被叫用户分配一个 MSRN，并将此号码送至 HLR，HLR 收到后再发送给 GMSC，GMSC 根据此号码选路，将呼叫接至被叫用户目前正在访问的 MSC/VLR 交换局。路由一旦建立，此号码就可立即释放。这种查询、呼叫选路功能（即请求一个 MSRN 功能）是 No.7 信令中移动应用部分（MAP）的一个程序，在 GMSC-HLR-MSC/VLR 间的 No.7 信令网中进行传递。

MSRN 的结构和 MSISDN 完全一致，如图 4.52 所示。

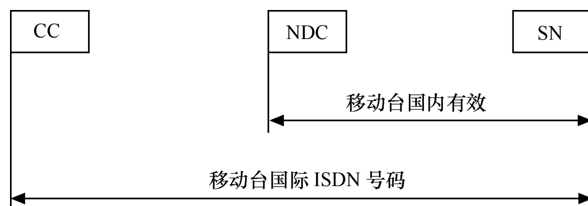


图 4.52　MSRN 的组成

为了让读者完全理解 MSISDN、MSRN 以及 IMSI 之间的关系，下面用两个手机之间呼叫建立的一组图来展示，如图 4.53～图 4.59 所示。

图 4.53 所示为手机 A 起呼，和 MSC-1 建立连接的过程。

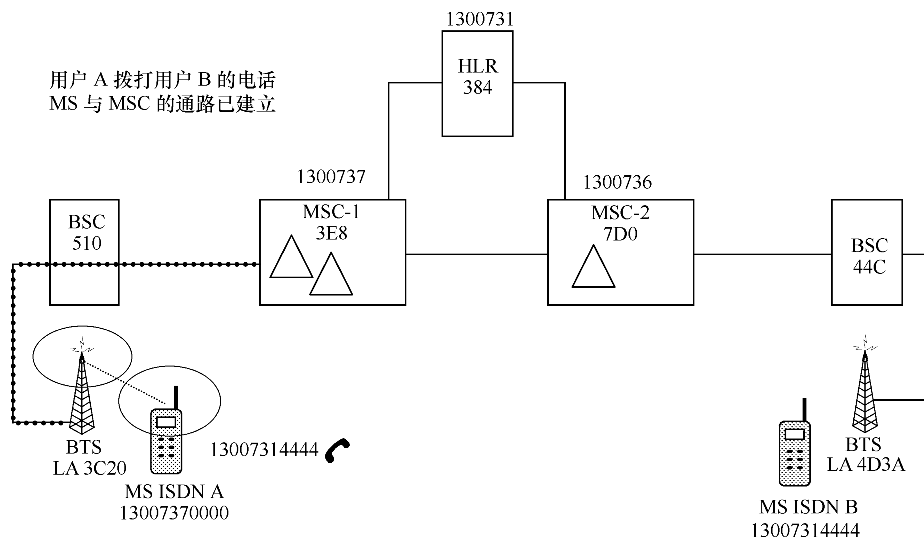


图 4.53　呼叫建立



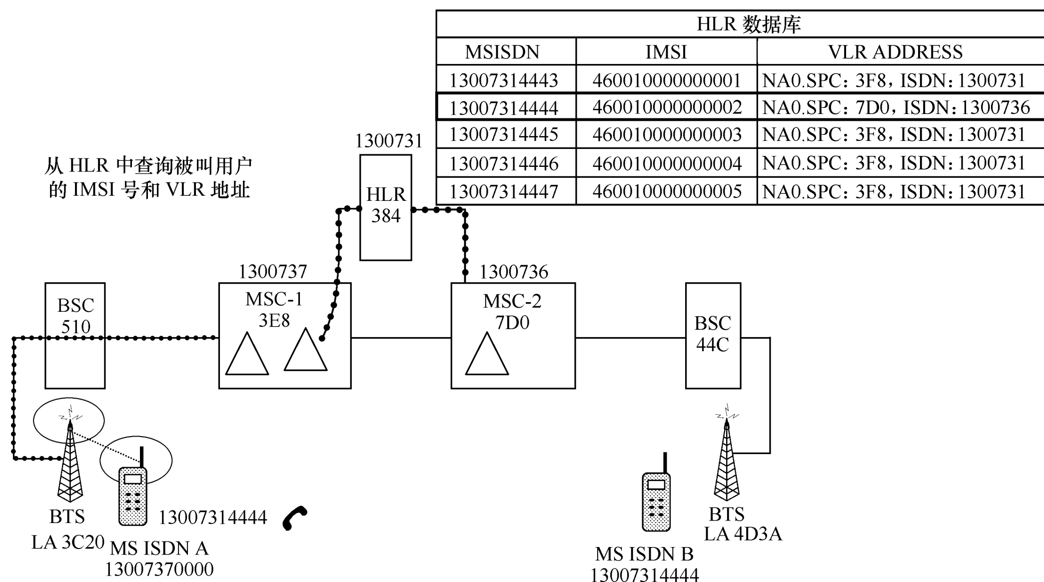


图 4.54　查询 IMSI 和 VLR 地址（注：IMSI 非真实，仅为说明情况）

建立连接后，MSC-1 查询被叫用户 13007314444 的 HLR，得到被叫用户的 IMSI 和 VLR 地址。

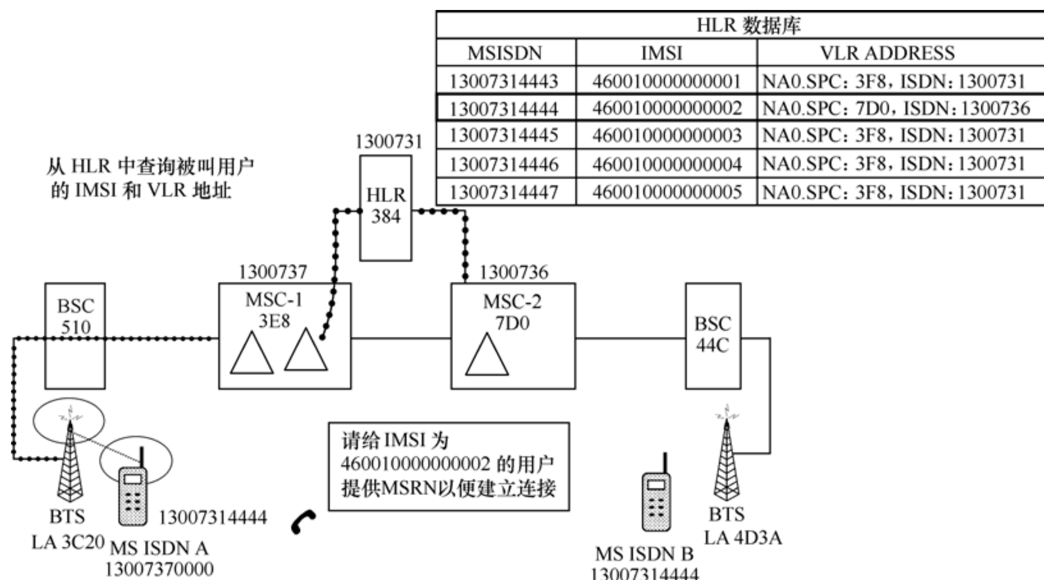
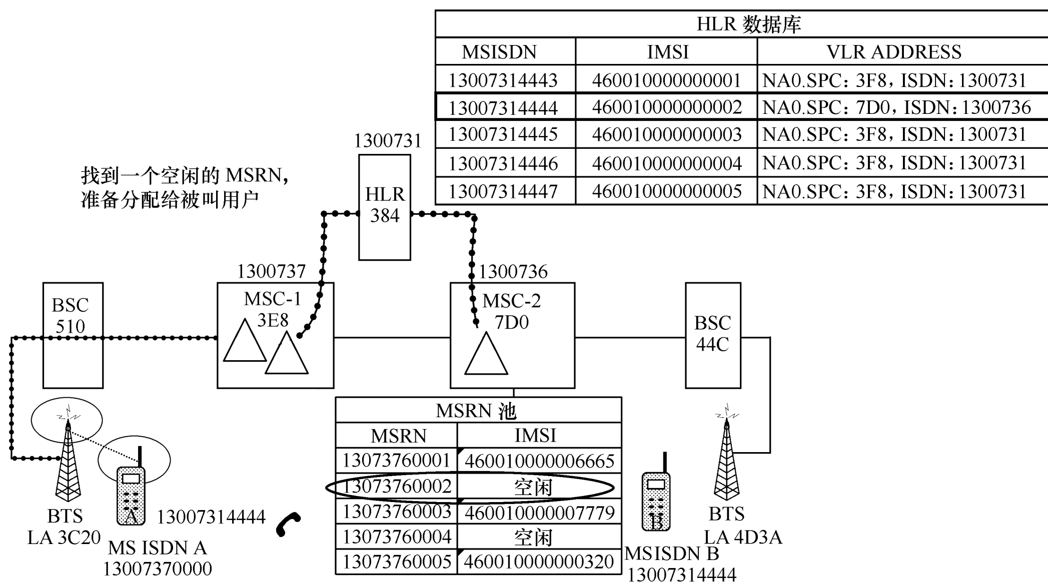


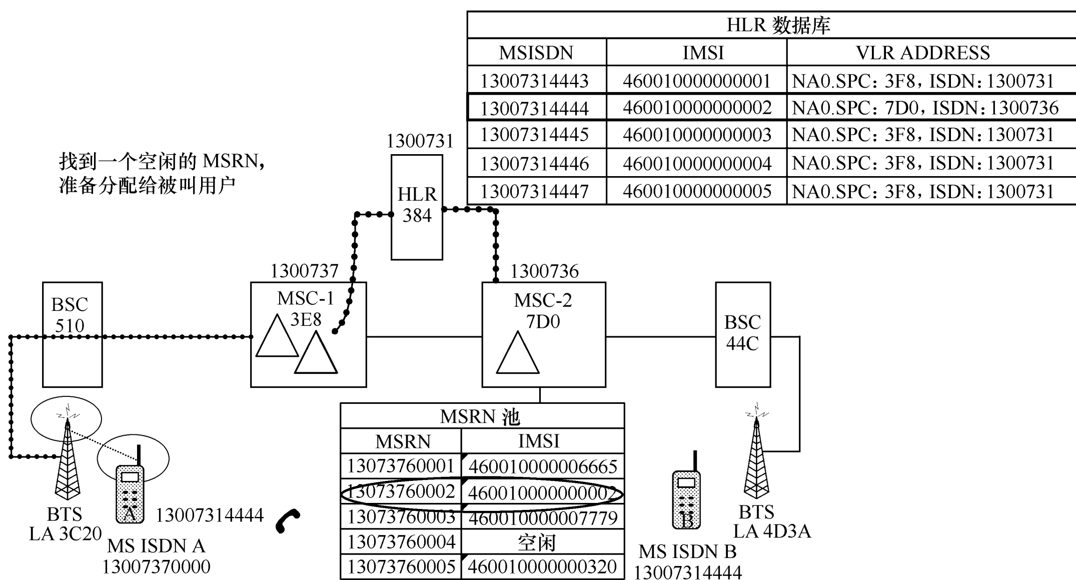
图 4.55　要求 MSC-2 提供一个 MSRN 给 HLR



HLR 数据库		
MSISDN	IMSI	VLR ADDRESS
13007314443	460010000000001	NA0.SPC：3F8，ISDN：1300731
13007314444	460010000000002	NA0.SPC：7D0，ISDN：1300736
13007314445	460010000000003	NA0.SPC：3F8，ISDN：1300731
13007314446	460010000000004	NA0.SPC：3F8，ISDN：1300731
13007314447	460010000000005	NA0.SPC：3F8，ISDN：1300731

MSRN 池	
MSRN	IMSI
13073760001	460010000006665
13073760002	空闲
13073760003	460010000007779
13073760004	空闲
13073760005	460010000000320

图 4.56　找到一个空闲的 MSRN



HLR 数据库		
MSISDN	IMSI	VLR ADDRESS
13007314443	460010000000001	NA0.SPC：3F8，ISDN：1300731
13007314444	460010000000002	NA0.SPC：7D0，ISDN：1300736
13007314445	460010000000003	NA0.SPC：3F8，ISDN：1300731
13007314446	460010000000004	NA0.SPC：3F8，ISDN：1300731
13007314447	460010000000005	NA0.SPC：3F8，ISDN：1300731

MSRN 池	
MSRN	IMSI
13073760001	460010000006665
13073760002	460010000000002
13073760003	460010000007779
13073760004	空闲
13073760005	460010000000320

图 4.57　分配 MSRN

应当说这还不是一个呼叫的完整过程，呼叫信息送至 MSC-2 后，MSC-2 会送至 BSC，由 BSC 进行寻呼，最后建立用户 A 和用户 B 的连接，这些内容我们会在信令流程中加以详述，这几幅图已经足以揭示 MSISDN、MSRN 和 IMSI 之间的联系和区别了。



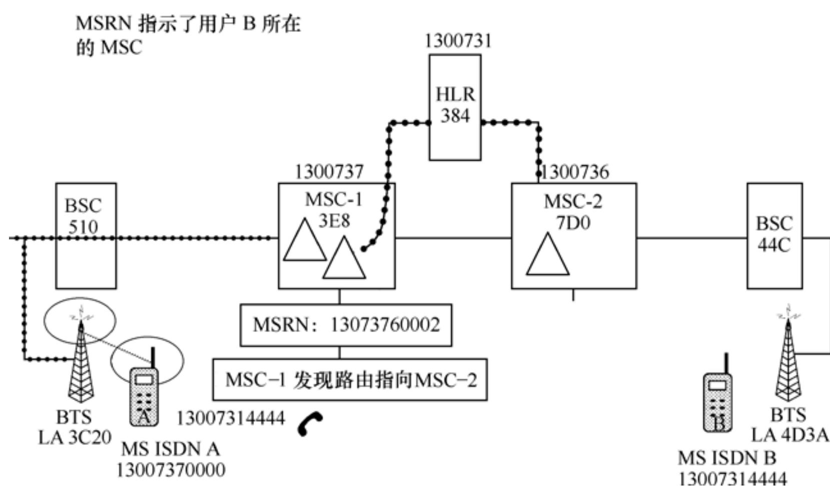


图 4.58　HLR 返回 MSRN 结果

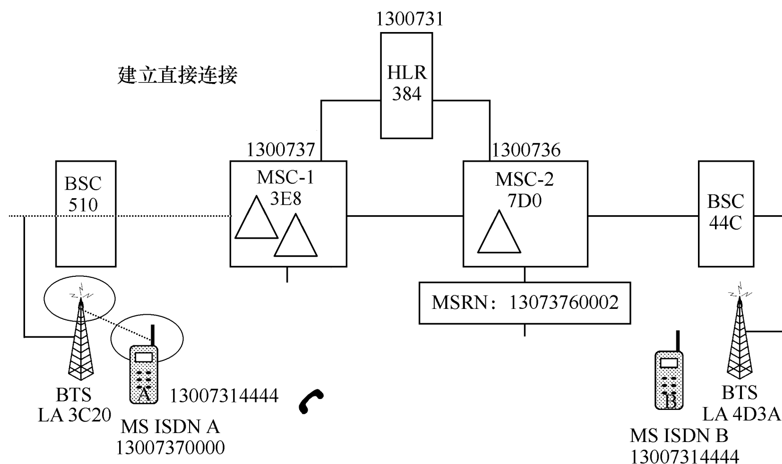


图 4.59　MSC-1 和 MSC-2 建立直接连接

4. 切换号码（HONR）

HONR 是用来建立切换所涉及的两个 MSC 之间的话路连接的，它是由目的 MSC 收到切换源 MSC 的切换请求后分配给这次切换的，它可看作是 MSRN 的一部分，组成和 MSRN 相同。

5. 临时移动用户识别码（TMSI，Temporary Mobile Subscriber Identity）

TMSI 是为了对用户身份进行保密，而在无线通道上代替 IMSI 使用的临时移动用户标识，这样可以保护用户在空中的话务及信令通道的隐私，它的 IMSI 不会暴露给别人。它是由 VLR 分配给在其覆盖区内漫游的移动用户的标识码，和用户的 IMSI 号相对应，

只在本地 VLR 内有效，TMSI 可用作位置更新、切换、呼叫、寻呼等操作时的用户识别码，并可在每次鉴权成功之后被重新分配，该号只在本 MSC 内有效。

6. 国际移动台设备识别码（IMEI，International Mobile Equipment Identity）

在国内，由于没有给移动台鉴权用的 EIR，这个识别码一般用得很少。该识别码用于唯一地识别一个移动台设备，而与使用该手机的 SIM 卡用户无关。在用户不用 SIM 卡作紧急呼救时，IMEI 可被用作用户标识号码，这也是唯一的 IMEI 用于呼叫的情况。各位可以试试，不插 SIM 卡也是可以拨打 110 等紧急电话的。

如图 4.60 所示，IMEI 的组成结构如下：

IMEI＝TAC+ FAC+SNR+SP

TAC＝型号批准码，由欧洲型号认证中心分配。

FAC＝工厂装配码，由厂家编码，表示生产厂家及其装配地。

SNR＝序号码，由厂家分配，识别每个 TAC 和 FAC 中的某个设备的。

SP＝备用，备作将来使用。

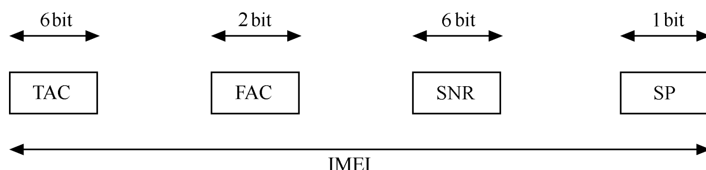


图 4.60 IMEI 号

7. 位置区识别码（LAI）

LAI 代表 MSC 业务区的不同位置区（如图 4.61 所示），用于移动用户的位置更新，其号码结构是：

LAI=MCC+MNC+LAC

MCC＝移动用户国家码，用于识别一个国家，同 IMSI 中的前 3 位数字。

MNC＝移动网号，用于识别国内的 GSM 网，同 IMSI 中的 MNC。

LAC＝位置区号码，用于识别一个 GSM 网中的位置区，LAC 的最大长度为 16bit，在一个 GSM PLMN 中可定义 65 536 个不同的位置区。

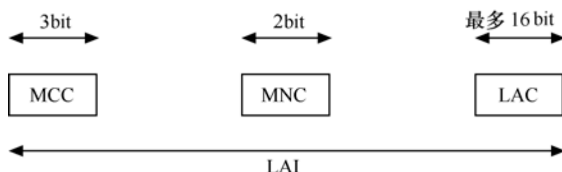


图 4.61 LAI 号



8. 全球小区识别码（CGI）

CGI 用来识别一个位置区内的小区，一个位置区有若干个 BTS，每个 BTS 一般有 3 个位置区。它是在位置区识别码（LAI）后加上一个小区识别码（CI，Cell Identity），如图 4.62 所示，其结构是：

CGI＝MCC+MNC+LAC+CI

MCC＝移动用户国家码，用于识别一个国家。

MNC＝移动网号，用于识别国内的 GSM 网。

LAC＝位置区号码（在一个 GSM PLMN 中，可定义 65 536 个不同的位置区）。

CI 是小区识别代码。

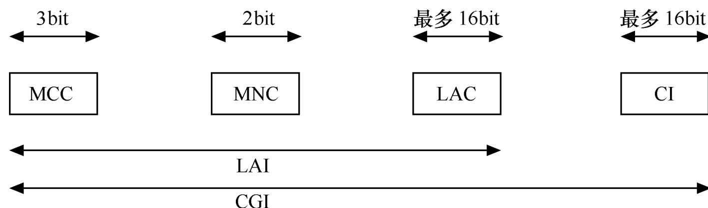


图 4.62　CGI 号

9. 基站识别码（BSIC）

基站识别码有点特殊，它有一点与上面的识别号都不同，那就是它不是唯一的，它的位数很短，数量也很少。其主要目的是用于移动台识别相邻的、采用相同载频的、不同的基站收发信机（BTS）。在网络优化上，同频同 BSIC 是大忌，这很容易导致切换失败。

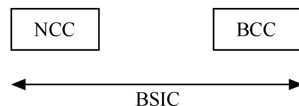


图 4.63　BSIC 号

如图 4.63 所示，BSIC 为一个 6bit 的编码，其结构如下：

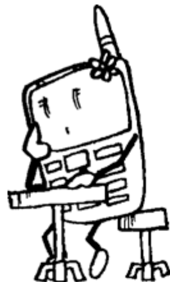
BSIC=NCC+BCC

NCC 是网络色码，用于识别 GSM 移动网。

BCC 是基站色码，用于识别基站。

第5章

Chapter 5



源于频率的困惑——GSM空中接口物理层的设计

通过第 4 章的学习，我们对 GSM 设备以及网络的整体构架有了一定的了解，本章我们开始要学习一些底层的东西。从本章开始直到第 7 章，我们都会围绕物理层、数据链路层和网络层进行学习，应当说这部分的内容很多、很复杂，但是难度并不大，我们在学习的时候应该多进行类比，以加深记忆。到了第 8 章，我们会把第 5～7 章的内容串起来，系统地了解 GSM 的信令流程。

我们在 3.1 节中反复强调，空中接口的频率资源是极其有限的，对于运营商而言是最宝贵的战略资源。资源因为稀缺，就要精打细算，加强管理，这一点在 GSM 空中接口物理层的设计上体现得淋漓尽致。就国内而言，银行的窗口资源也是稀缺的，我们去银行也是经常要排队的，银行业采取了多种措施来提高资源的利用效率，比如营业厅的引导员——先询问你要办理什么业务，然后指引你到相应的窗口，这与 GSM 中 SDCCH 的功能就有些类似；比如说用大屏幕展示银行的业务信息，让你办理业务的时候就心中有数——这与 GSM 空中接口的 BCCH 也颇有异曲同工之妙。我们希望尽量多地找到这种相似之处，这不仅有利于我们对问题的理解，也有利于对知识点的记忆。

空中接口的种种信道的设计，就其本质而言，都是为了提高频谱资源的利用效率。仔细研究它的设计理念就会发现，空中接口物理层的这种设计方式，管理学层面的东西比纯技术层面的东西要更多。

下面我们就开始学习 GSM 空中接口的物理层，首先从物理信道开始，了解突发脉冲、时隙、TDMA 帧的概念，这都是 GSM 网络中最基础的内容，非常重要，请不要因为它简单就忽略了；然后了解逻辑信道，逻辑信道也分为业务信道和控制信道。请注意，



这里讲的逻辑信道是 GSM 物理信道的映射，同样属于物理层的范畴，因为它只需要考虑如何给各种信息提供一条合适的空中通路，而并不需要考虑如何确保完成点对点通信的有效传输，所以不要把它归到数据链路层了。

5.1 TDMA空中接口技术

对于时分多址（TDMA，Time Division Mutiple Access），应该并不陌生，我们曾在 3.1.4 节中就这个问题进行过一番水煮，相信大家应该还有印象。下面就这个问题进行更为详细的叙述。

TDMA 是在一个宽带的无线载波上，按时间（或称为时隙）划分为若干个时分信道，每一用户占用一个时隙，只在这一指定的时隙内收发信号，故称之为时分多址，如图 5.1 所示。

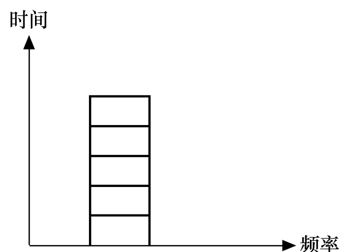


图 5.1　TDMA

GSM 是 FDMA 与 TDMA 的混合，不但有时分，也有频分。另外，GSM900 的上行链路和下行链路是频分的，它的上行频段为 890～915MHz，下行频段为 935～960MHz，上下行运行在不同的频段，BTS 需要通过双工器来区分上下行，俗称频分双工。而像 PHS 和 TD-SCDMA 这样的 TDMA 系统就不同了，它们的上下行都运行在同一个频段上，通过在不同的时间里工作来区分上下行，俗称时分双工，时分双工是不需要双工器的。

GSM 移动用户开始呼叫时，GSM 网络为用户分配一个时隙，用户与基站之间进行同步通信，并对时隙进行计数。当自己的时隙到来时，手机就启动接收和解调电路，对基站发来的突发脉冲进行解码。同样，当用户需要发送信息时，首先对信息进行缓存，等待自己的时隙的到来。在时隙开始后，将存储的信息发送出去，然后又开始积累比特信息流等待下一次突发脉冲的发送。

1. 突发脉冲与时隙

GSM 在无线路径上的传输单位是由 GMSK 调制的比特组成的脉冲串，称为“Burst”——突发脉冲。突发脉冲的长度有限——只有 156.25bit；占据的频谱有限——每时隙所占的频谱资源只有 200kHz，要不怎么叫频分呢。所谓频分就是把 25MHz 的频段切成每条 200kHz 给你们分。

突发脉冲在一个时间和频率的窗口上发送，这个窗口称为“time slot”——时隙。时隙的中心频率位于系统频带为 200kHz 的间隔上，并以 0.577ms 的时间重复，精确一点

说，是以 15/26ms 重复。这个由频域和时域组成的空间“time slot”，就是 FDMA 和 TDMA 在 GSM 中的应用，如图 5.2 所示。

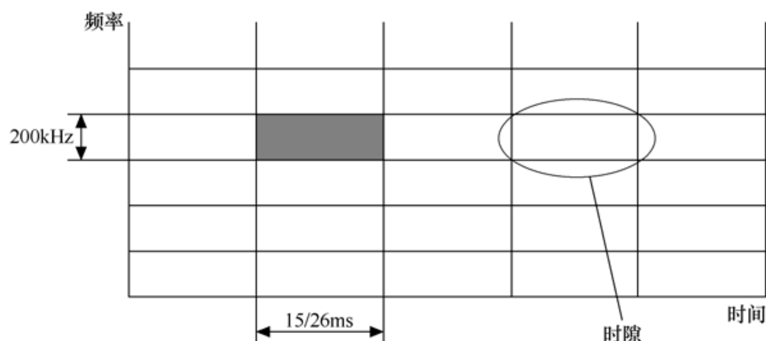


图 5.2　时隙

突发脉冲在一个时隙上发送，那么突发脉冲的格式是怎样的呢？

TDMA 信道上一个时隙中的信息格式称为突发脉冲序列。

突发脉冲序列分为 5 种类型：普通突发（NB，Normal Burst）脉冲序列、空闲突发（DB，Dummy Burst）脉冲序列、频率校正突发（FB，Frequency Correction Burst）脉冲序列、同步突发（SB，Synchronization Burst）脉冲序列和接入突发（AB，Access Burst）脉冲序列。我们会在后面详细讲述这些脉冲的应用，这里先介绍突发脉冲的结构。

突发脉冲的立体示意图和平面示意图如图 5.3 和图 5.4 所示。

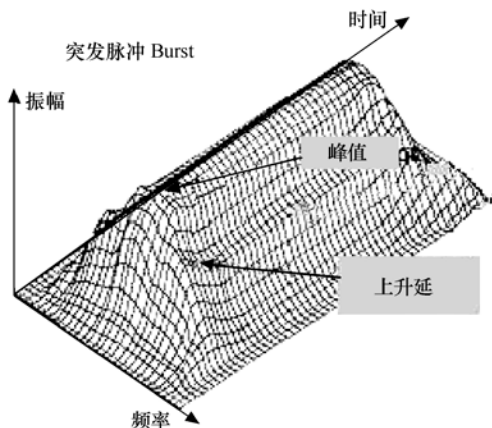


图 5.3　突发脉冲立体示意图

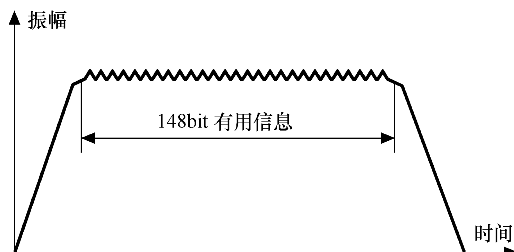


图 5.4　突发脉冲平面示意图

（1）普通突发脉冲序列

普通突发脉冲序列用于携带业务信道（TCH）及除 RACH、SCH、FCCH 控制信道



上的信息。RACH、SCH 和 FCCH 出于各自的考虑，其组成格式与突发脉冲序列有所不同。普通突发脉冲序列的格式如图 5.5 所示。

尾比特 3bit	加密比特 57bit	Flag 1bit	训练序列 26bit	Flag 1bit	加密比特 57bit	尾比特 3bit	保护间隔 8.25bit

图 5.5　普通突发脉冲序列

TB（Tail Bit）是尾比特的意思，TB 的数值总是 000，以帮助均衡器识别起始位和终止位。普通突发脉冲序列有一个 26bit 的训练序列，这是一串特定的比特序列，共有 8 种。BTS 在设置 BSIC 号的时候，相应的比特序列也就设置了。其作用是帮助均衡器产生和修正信道模型，以消除时间色散，我们在 3.2.5 节中对这个问题有过描述。

GP（Guard Period）是保护间隔，共 8.25bit，大约 30ms，这是一段空白信息，防止有时隙交错时，有用的比特信息不会交错，相当于高速上行车与行车之间的安全距离，要是一辆车出了一点小状况，后面的车有这个安全距离就不至于发生状况。我们在 3.2.4 节中提过，手机发射信号是需要测算传播时间然后给予一个提前量的，但是这不一定非常精确，时隙和时隙之间有微小的滑动是完全可能的，采用保护带之后，允许有一小段空白的时间误差，这在一定程度上降低了定时精确性的要求。准确地说，时隙的长度是 0.577ms，脉冲序列的长度是 0.546ms，允许时隙中突发脉冲序列有 0.031ms 时间上的误差，因此 8.25bit 的保护可以使发射机有一定的余地。

Encrypted bit 是加密比特的意思，语音信号经过 A5 算法加密后就填充进了上述两段比特信息中，每段 57bit。F 是借用标志的意思，打电话的时候，我们一直占用的是 TCH，信令都没地方传了，如果出现了比较紧急的信令要传递，比如说切换信息，那就把两个 F 位“偷帧信号”置为 1，说明此时突发脉冲序列已经被 FACCH 信令借用。如果只设置了一个比特，表示突发脉冲序列只有一半被盗用。其中，“0”表示是 TCH，“1”表示是 FACCH。

（2）频率校正突发脉冲序列

该突发脉冲序列传送下行的 FCCH，使 MS 能校正自己振荡器的频率并锁定到 BTS 的频率，它相当于一个特定频率的未调制的载波在 FCCH 上发送。频率校正突发脉冲序列如图 5.6 所示。

TB 3bit	固定比特 142bit	TB 3bit	GP 8.25bit

图 5.6　频率校正突发脉冲序列

可以看出，频率校正突发脉冲序列也有前后各3bit的尾比特和8.25bit的保护比特，其作用和普通突发脉冲序列相同。142个固定比特全为0，这个信息很特殊，便于MS一眼识别并锁定载波频率。

可以发现，相比普通突发脉冲序列，这里少了训练序列和偷帧位。训练序列是不需要的，现在还没有建立连接，MS还处在锁频的过程中，根本就没有信息交换，要信道模型何用？偷帧位也是不需要的，MS锁定载频前连BCCH广播信息都听取不了，更谈不上其他信令，因此这个也可以不要。

（3）同步突发脉冲序列

同步突发脉冲序列用于MS和BTS间的时间同步，这里含有一个长同步序列已经TDMA帧号（FN，Frame Number）以及基站识别码（BSIC）的相关信息。同步突发脉冲序列在SCH上发送。

尾比特 3bit	加密比特 39bit	同步序列 64bit	加密比特 39bit	尾比特 3bit	保护间隔 8.25bit

图5.7　同步突发脉冲序列

可以看出，同步突发脉冲序列包含前后各3bit的尾比特（TB），8.25bit的保护空间。与突发脉冲序列有所不同的是，它有长达64bit的同步序列。这个同步序列是固定的，也可以看作是训练序列，此时网络还未建立连接，需要更多的比特位用于信道均衡来确保信息传递的有效性。78bit的加密比特也有其特定的出处，我们在3.2.1节的信道编码中已经对这个问题有所叙述，就不在这里重复了。

（4）接入突发脉冲序列

接入突发脉冲序列用于MS的随机接入。这种突发脉冲序列设置了一个较长的保护间隔（GP），所以其有用信息比其他类型的脉冲序列短很多。因为MS试图接入到系统时还不知道发射定时，所以要增加保护带。MS发送该突发脉冲序列时，BTS并不知道MS的位置，所以来自MS的消息的定时也无法准确计算（接入突发脉冲序列仅为上行）。由于第一个突发脉冲序列中没有时间调整，MS接入与后一个串有一定的交错，基站可以根据交错码个数来计算TA值。

尾比特 3bit	同步序列 41bit	加密比特 36bit	尾比特 3bit	保护间隔 68.25bit

图5.8　接入突发脉冲序列

（5）空闲突发脉冲序列

在其他信道不发送突发脉冲序列时，基站收发信机须在小区配置中C0的下行



信道的每个时隙发送一个突发脉冲。因为 MS 是要不断监视 BCCH 射频的功率的，以便于进行小区选择。如果 BCCH 载频的 TCH 时隙有时候不发送信号，就会影响周围的 MS 对该载频信号强度的评估，因为评估信号强度是根据采样点取平均值而得来的。

所以如果有 BCCH 载频的时隙处于空闲状态，那就要发送空闲突发脉冲序列，不能让它闲着。空闲突发脉冲序列的结构如图 5.9 所示。

尾比特 3bit	加密比特 58bit	训练序列 26bit	加密比特 58bit	尾比特 3bit	保护间隔 8.25bit

图 5.9　空闲突发脉冲序列

2. TDMA 帧

在 GSM 的 TDMA 中，每个载频被定义为一个 TDMA 帧，每个帧包含 8 个时隙（TS0～TS7），需要定义 TDMA 帧号。TDMA 帧号需要用来做 MS 与 BTS 的同步以及语音信号的加密，同步用在 SCH 上，加密是和 Kc 以及原始信号一起通过 A5 算法进行的。

然后有了 TDMA 帧号，MS 也可以判断当前载频到底是 BCCH 载频还是 TCH 载频，它的 0 号时隙传递的到底是 BCCH 信号还是 TCH 信号。因为 BCCH 载频包含了 SCH，SCH 告知了 BCCH 的 TDMA 帧号，因此载频的性质是可以根据 TDMA 帧号来分辨的。

说到 TDMA 帧，不能不说复帧，复帧是针对 TDMA 帧中的一个特定时隙来定义的，这是什么意思呢？看下面的图 5.10 和图 5.11 就明白了。

GSM 规范定义了两种不同的复帧结构，即含 26 帧持续时间为 120ms 和含 51 帧持续时间为 235.8ms 的两种。这两种帧都有各自的用途。

（1）26 帧的复帧

26 帧的复帧包括 26 个 TDMA 帧，持续时间为 120ms，一般用于 TCH（以及跟随 TCH 的 SACCH 和 FACCH），作为话音信道及其随路控制信道。

在 26 帧业务信道复帧中，帧 12（帧从 0 号帧算起，所以是第 13 帧）被用作慢速随路控制信道（SACCH），用来在 MS 和 BTS 之间传送链路控制信息。小区给每个业务信道分配的时隙都是这种格式，也就是说，最开始是 12 个突发脉冲序列的业务信息，接下来是 1 个 Burst 的 SACCH，然后是 12 个 Burst 的业务信息和一个空闲的 Burst。

当采用半速率时，26 帧业务复帧中每个用来传业务的帧可以传两路 MS 用户通话（空中接口中 MS 的数据速率是原来的一半）。尽管业务数据速率减半了，但 SACCH 信息没有少，所以要把原来空闲的帧 25 也用作 SACCH。图 5.10 就是一个典型的 26 帧复帧。

图 5.10　26 帧的复帧

（2）51 帧的复帧

51 帧的复帧包括 51 个 TDMA 帧，持续时间为 235.385ms。这种复帧用于携带 BCH 和 CCCH，专用于控制信道。

我们注意到，26 和 51 是没有公约数的，将 BCH 和 TCH 的复帧数设置成这样特别的数字是有其深意的，后面会为大家说明。图 5.11 就是一个典型的 51 帧复帧。

（3）超帧（Superframe）

我们知道，51 帧和 26 帧之间是没有公约数的，要设置一种帧可以容纳这两种帧，那么这个帧的容量就必须要达到 51×26=1 326 帧。这种帧称为超帧，1 326 个 TDMA 帧相当于 6.12s 的时间。



图 5.11　51 帧的复帧

（4）巨帧（Hyperframe）

除了超帧之外，人们还定义了巨帧，一个巨帧包含了 2 048 个超帧结构。巨帧结构含 26×51×2048=2 715 648 个 TDMA 帧，持续时间为 3h28min53s760ms。每个 TDMA 帧由帧计数器（FN）来标记。这些 TDMA 帧按照顺序排列，依次从 0 到 2 715 647，帧号在同步信道中传送。

巨帧也与加密和跳频有关系，一个巨帧持续 3 个多小时，每当一个新的巨帧开始时，加密和跳频算法也重新开始。

帧（Frame）、复帧（Mutipleframe）、超帧（Superframe）、巨帧（Hyperframe）之间的关系如图 5.12 所示。

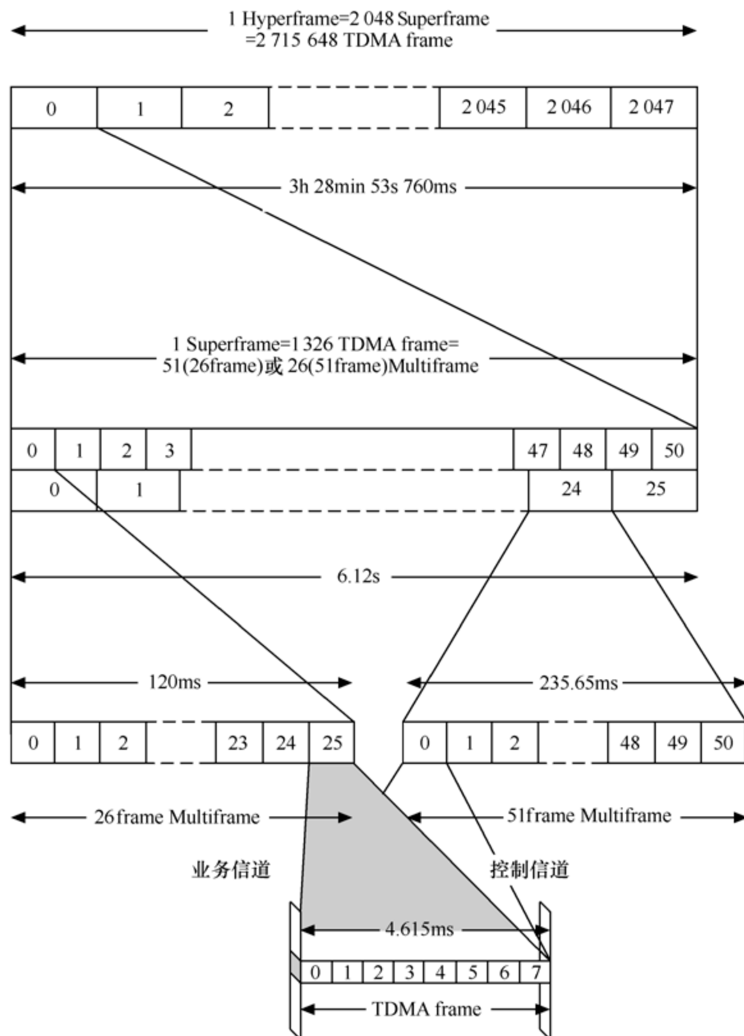


图 5.12 帧—复帧—超帧—巨帧

5.2 铁路的管理艺术——突发脉冲的应用

我们在上一节中对突发脉冲序列以及 TDMA 复帧的结构作了一番介绍，不过并没有解释它们的具体用法，那么下面就要来完成这项工作。GSM 的突发脉冲具体的有十几种，看起来会增加基站收发信机结构的复杂程度。然而，每种脉冲都有其存在的意义和价值，都是为了提高空中接口的频谱资源利用效率，当然，除了效率之外，也有一个通信质量



方面的需要。所以我们说，空中接口的物理层之所以设计得这么复杂，与其说是一个技术的问题，还不如说是管理的需要。

TDMA 帧分配给 MS 一个时隙，该时隙称为 GSM 物理信道。突发脉冲序列都在时隙上传送，也就是在物理信道上传送。当同一个物理信道承载不同的突发脉冲时，它就成了不同的逻辑信道。当它承载 TCH 脉冲时，它就是业务信道；当它承载 BCCH 脉冲时，它就是广播信道；当它承载 SCH 脉冲时，它就是同步信道。

我们可以把物理信道和逻辑信道的关系看成是铁路与火车的关系，铁路只是载体，铁路上跑的内容取决于你用的是什么火车。你要用货车那就是货运，你要用客车那就是客运。有人说物理信道与逻辑信道是映射关系，我觉得说成是承载关系或许更有利于理解。

逻辑信道粗略地可以划分为两种：业务信道（TCH）和控制信道（CCH）。这种划分很好理解，在当年看来也很清晰，如今界限就稍微显得有点模糊。TCH 是用于语音通话的，是业务信道那自不必说；然而 SDCCH 和 SACCH 这两种专用控制信道也可以传送短消息，你能说它们就不是业务信道？可能是因为 GSM 的设计者没想到短信业务的发展是如此迅猛吧，但这并不会对我们理解概念造成多大的妨碍，因为 SDCCH 和 SACCH 主要还是用来传递信令的。

在深入了解每个具体的信道的功能之前，我们先得知道有多少种信道。对于业务信道而言，没有太多可说的，它有好几种信道，不过不同的信道之间除了速率不同以外，其他都是一样的。

控制信道就要复杂得多，我们先来看看控制信道的列表，如图 5.13 所示。

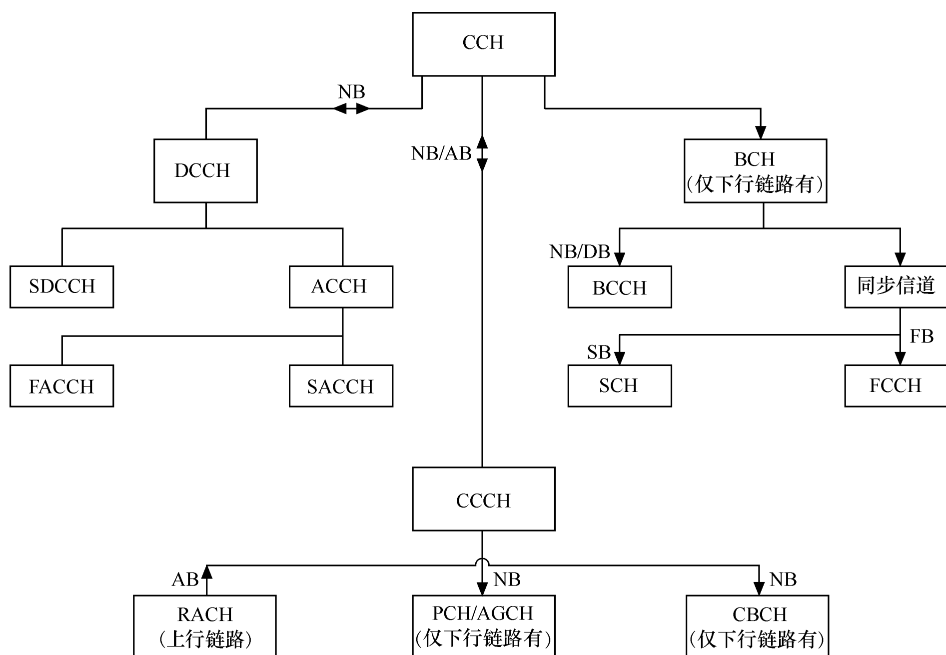


图 5.13　控制信道

5.2.1　客运火车——业务信道（TCH）

手机是用来通话的，那么对于 GSM 而言，最关键的信道当然是业务信道了。好钢要用在刀刃上，有限的资源要用在最赚钱的地方，这就是运营商的逻辑。TCH 也占了所有物理信道的绝大部分。

你可以把 TCH 理解为铁路局的客运火车，TCH 是用来承载语音信息流的，客运火车是用来承载客流的，两者颇有类似之处。客运火车当然是铁路局最宝贵的资源，要好好利用。

TCH 根据发送速率的不同，分为全速率语音信道（TCH/F）和半速率语音信道（TCH/H），全速率语音信道的传输速率为 22.8kbit/s，半速率语音信道的传输速率为 11.4kbit/s。

全速率语音信道上可以有两种不同的编码方式，第一种就是常见的语音编码，称为 TCH/FR（Full Rate），语音信源编码后速率为 13kbit/s，经过信道编码后速率为 22.8kbit/s；第二种称为增强型语音编码 TCH/EFR（Enhanced Full Rate）。语音编码后速率为 12.2kbit/s，经过信道编码后速率也是 22.8kbit/s。EFR 采用了一种新的语音编码算法，可以提供更好的语音质量。

除此之外，TCH 也可以传递数据业务，速率分别为 9.6kbit/s、4.8kbit/s、2.4kbit/s，可以用 TCH/9.6、TCH/4.8、TCH/2.4 来表示。

我们把上述内容归纳一下，如图 5.14 所示。

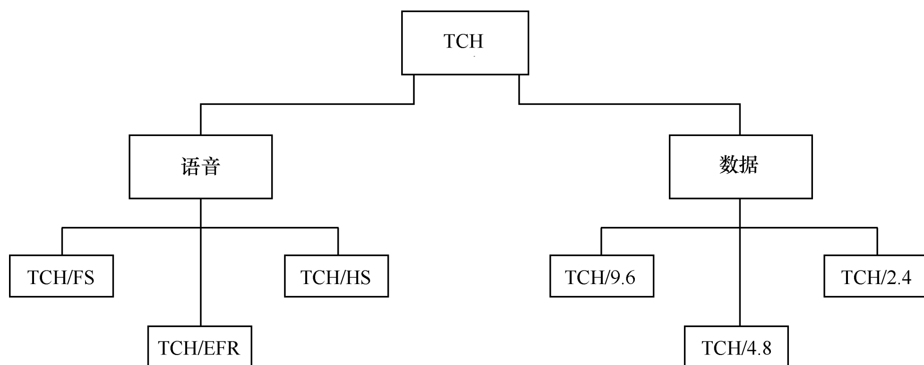


图 5.14　TCH

5.2.2　候车厅的大喇叭——FCCH

话说运营商虽然目前主要的赢利手段就是 TCH，但是也不能只搞 TCH 就不搞别的



信道了。TCH 就像马路一样，作为交通局，你不能光修好马路就认为这条马路可以跑车了，还得有红绿灯，还得有交警，还得有监控摄像头。凡是有资源的地方就得有控制，要不大家争抢资源就会没了规矩，乱了套，最终会降低资源的使用效率。

为了提高 TCH 的使用效率，也为了 TCH 能够正常使用，GSM 的设计者狠狠心腾出了一部分物理信道来跑控制信息。

对于火车站来说也是如此，咱不能光考虑修铁路开火车，各种配套措施和监控措施也是一定要跟上的，要不大家都乱哄哄地挤火车，那还了得。

我们走到火车站的候车大厅时，经常会听见一个大喇叭在那里咿咿呀呀地喊叫，有时还放一下流行歌曲。这都没关系，这个喇叭很多时候的功效就是吸引你的注意力，锁定你的眼球，省得它说正经事的时候你把它给忽略了。

FCCH 的功效也类似于此，它下发一个长达 142 位的全 0 比特，这个比特这么特殊，就是为了让 MS 校正自己的振荡器的频率并锁定到该 BTS 的频率。只有锁定了该块载频，MS 才能收听到跟随在 FCCH 之后的同步信息 SCH 和 BCCH。FCCH 是点对多点传播的（BTS 对多个 MS），这与大喇叭完全一致。

应该说 FCCH 的作用比大喇叭来得更重要，因为对于人类这种高级智能生物，即使没有竖起耳朵注意锁定该喇叭的播放信息，有时偶尔也能听到飘过耳边的一点重要信息。但是对于手机这种笨家伙来说，那就完全不行了，它必须把频率调谐到该 FCCH 所在载波的频率，才能完成后面的工作，要不你就啥也别指望它干了。

FCCH 的目的有两个：一是确认这是一个 BCCH，只有 BCCH 才有 FCCH 信息，FCCH 只在下行的 BCCH 载频的 0 号时隙上传送；二是保证手机的频率和 BTS 一致，也就是锁频。

5.2.3　现在是北京时间八点整——SCH

大喇叭成功地吸引你的注意力后，就要开始干点别的了。它首先要干的工作就是报时：“旅客朋友们，现在是北京时间八点整——北京西客运火车站为您播报。”

报时这活对于一个火车站来说是必须的，这年头谁的手表快个几分钟慢个几分钟是谁也说不准的事情，对于赶火车而言，误了时间是要命的，过了这村可没这店，赶不上趟您就准备在候车大厅打地铺好了。既然锁定您的注意力了，那别的事情咱先别干，咱校对校对时间先。

时间校准那是应该的，可这火车站咋还打广告呢。您瞧，还报个啥“北京西客运火车站为您播报”，这可不地道啊。嗨，这可不是广告，它要不说这是西客运火车站你咋知道这是西客站呢，要是南客站或者北客站您不坐在这里白等了吗。

SCH 也类似于此，SCH 携带 MS 的帧同步信息（TDMA 帧号）和 BTS 的识别码（BSIC）

的信息，用作下行信道，在 BCCH 载频的下行链路的 0 号时隙发送。

TDMA 帧号是用来 MS 和 BTS 之间同步的，有点类似于“八点整”那一嗓子。BSIC 号是用来识别基站的，BSIC 好歹是一个 6bit 编码，有 2^6=64 位信息，能给 64 个基站进行编码。这可比火车站强多了，火车站大概是一个 2bit 的编码，横竖只有 4 位信息：东、西、南、北。

5.2.4 “我的地盘，我的业务”——BCCH

不要认为那大喇叭报完时就消停了，这是不可能的，经还没念完呢。“高僧，请问您的经哪年哪月才能念完？”。“永生永世”——施主遂口吐白沫倒地不起。要指望 BCCH 载频有一刻不发送信息，那是不可能的，除非它倒下了，要不然就算 BCCH 载频上有话务信道时隙没有东西发送，它也要给你整个空闲突发脉冲序列塞个满满的。因为旁边的手机都在测试 BCCH 信号的强度，强度的测量是按所有采样点平均得来的，如果偷懒不发送信息，那个测量出来的电平值唰地一下就掉下去了，BCCH 载频和 BCCH 载频之间是要互相攀比竞争信号强度的，它可丢不起那人。

大喇叭还要广播哪些信息呢？

（1）位置区识别号（LAI）——这个信息对别人找你有帮助，也就是说，告诉你本火车站到底是位于海淀区还是丰台区。

（2）移动台应监视的相邻小区列表——你应该关注的相邻的火车站的列表，除了本火车站，旁边还有别的火车站，比如说南客站、北客站。如果本火车站爆满或者您对某些条件不太满意的话，不妨可以选择别的火车站。

（3）小区识别号——本火车站有好些站台，不同的站台叫做不同的小区，它们的编号可是不同的，别弄混了。

（4）本小区使用的频率列表——这就相当于客运线路列表了，告诉你都有多少列车，都是什么车次，别搭错了哦。

（5）接入控制——本火车站人满为患了，咱得控制人数，各位，把身份证拿出来啊，单号的可以买票，双号的请明天来，众皆哗然。

……

BCCH 与此类似，就是要向周围不断广播网络的信息，也称为系统信息。当移动台开机但没有通话时，会周期性地监视 BCCH 中的信息（至少每 30s）。除了监视移动台所驻守的小区的 BCCH 信息外，移动台还会监视相邻小区中的 BCCH 信息，并存储信号最强的 6 个小区的信息。这些小区的 SCH 信息也被存了下来，以便移动台到了一个相邻的新的小区后，可以快速与之同步（SCH 信息用来同步）。

那么 BCCH 都广播哪些信息呢？我们先来粗略地看一下：



① 位置区识别号（LAI）;
② 小区识别号（CGI）;
③ 本小区使用的频率列表;
④ 邻近小区描述;
⑤ 随机接入控制信息;
⑥ 小区选择参数;
⑦ 控制信道描述;
⑧ 小区选项。

BCCH 包含的系统信息很多，上述所列内容一时之间也很难弄明白是什么意思，等我们学完第 8 章信令流程再回过头来看就不难了。

5.2.5　想上车，请先买票——RACH/AGCH

听着大喇叭婆婆妈妈讲了一大堆，相信大家早已不耐烦了。俺不听你废话了，俺要上车，上列车！于是你大步流星地直奔检票口而去，结果被保安拦住了："哥们，车票呢，没买票就想上车啊，你当是公交车啊，门都没有"。

这就是列车与公交车的区别了，市内公交资源相对而言比较丰富，不需要提前买票搞预订制。而火车就不同了，在中国，由于地区间经济状况的差异，沿海发达地区与内地之间总是有庞大的客流，因此火车的资源总是显得很紧张，就必须得实行预订制——买票。不同的资源状况造就了不同的管理手段。而我们无线通信空中接口的频率资源永远是很紧张的，永远是不够用的，起码从目前人类的认知而言是这样的。那么占用 TCH 之前要先进行申请，这是必须的！

在 GSM 中，这个属于通用控制信道（CCCH，Common Control CHannel）的内容。CCCH 用于在 BTS 和移动台之间传递控制信息，完成呼叫建立和寻呼功能。

大家请注意了，为什么 RACH、AGCH、PCH 属于通用控制信道呢？通用和专用是这样划分的，还未建立起连接的就称为通用，已经建立好连接的，单独占用一条信道的就称为专用。在 RACH、AGCH、PCH 之时，移动台尚未与网络建立起连接，尚未单独占用一条独立的信道用于通信，所以称为通用控制信道。

（1）随机接入信道（RACH，Random Access CHannel）

MS 通过此信道申请分配一个独立专用控制信道（SDCCH），可作为对寻呼的响应或 MS 主叫/登记时的接入。RACH 在上行 BCCH 载频的 0 号时隙上传送。

（2）允许接入信道（AGCH，Access Grant CHannel）

AGCH 用于为 MS 分配一个独立专用控制信道（SDCCH），AGCH 在下行 BCCH 载频的 0 号时隙上传送。

5.2.6 “×××，你的家属在广播室找你”——PCH

在火车站找人是很难找的，地方又大，人又多。不过也不是没有办法，那就是让他自动现身，而不是你去找他。怎么个自动现身法呢？那就是借助之前那个大喇叭了。火车站工作人员可以在广播室里吼上一嗓子：“×××，你的家属在广播室找你”，这人十有八九就能找到了。也不排除不能找到的情况，一般是两种情况：带着耳机在听音乐，或者是干脆在候车大厅睡着了，对外界的信号没反应，俗称为“关机”；二是干脆脱离了广播所能及的范围，比如去了洗手间或者是干脆出了火车站，俗称为“不在服务区”。

我们还得关注一个问题，就是×××这个叫法该如何定义，直接用姓名是不太妥的，同名同姓的人多了去了，要是来个一呼百应可不好玩。必须来个唯一性的定义，比如“××省××市××县（区）××街道××门牌号×××人”，这个寻人启事看起来有点让人晕。好在 GSM 中每个 MS 的定义都是唯一的，IMSI 号用来作寻呼不会发生混淆；就算是用 TMSI 号作为寻呼，那也没有关系，至少在重新分配 TMSI 号前该标识是唯一的，不会发生混淆。

（1）寻呼信道（PCH，Paging CHannel）

PCH 用于寻呼 MS（可以通过 IMSI、TMSI、IMEI 来寻呼移动台），PCH 在下行 BCCH 载频的 0 时隙上传送。

（2）小区广播信道（CBCH，Cell Broadcast CHannel）

PCH 消息是以位置区进行寻呼（其实也是广播）的，而 CBCH 消息是以小区来进行广播的，如图 5.15 所示。该信道用来传递需要广播到小区中所有移动台的信息。CBCH 用专用控制信道（SDCCH）来发送信息，但是通常被看作是通用信道，因为小区内所有的移动台都能收到它发送的信息。

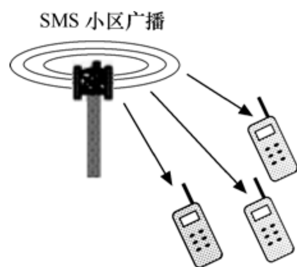


图 5.15　小区广播

5.2.7 列车导乘员——SDCCH

通常买票之后（RACH），并不会直接上火车（TCH），上火车之前要穿越那么多弯弯转转的走廊，很容易晕头转向。那么就需要一个列车引导员（SDCCH）引导你登上合适的站台，进入合适的火车。列车引导员（SDCCH）会先查看你票的真伪（俗称鉴权，没办法，这年头假票也很泛滥）和车次（你要坐什么火车，也可以理解为请求建立呼叫的原因），然后引导你上火车。

在 GSM 中，手机在建立连接之后也通常是先占用上 SDCCH 以和网络交换信息，等



待网络在 SDCCH 上下发立即指配命令后再占用 TCH。

SDCCH（Standalone Dedicated Control CHannel，独立专用控制信道）用在分配 TCH 之前在呼叫建立过程中传送系统信令，例如登记和鉴权在此信道上进行，空闲状态下的短消息和小区广播也在 SDCCH 上传送。运营商一般默认将 BCCH 载频的第 2 时隙用来传送 SDCCH。

在 SDCCH 上传送的信令消息和事件如下：

（1）位置更新（Location Updating）；

（2）周期性位置更新（Periodic Registration）；

（3）IMSI 分离与附着（IMSI attach/detach）——不妨先粗浅地理解为开关机；

（4）呼叫建立（Call setup）；

（5）点对点短消息（SMS，Short Message Service Point to Point）。

5.2.8　列车上的服务员——FACCH/SACCH

火车站的配套服务工作，并不是说上了列车（TCH）就万事大吉了，在列车上（TCH）上同样有很多服务工作需要做（控制信令需要传递）。

这些服务工作可以分为两类。

一类称为 SACCH，是慢速的、周期性的服务。所谓慢速服务，就是不需要立刻执行的服务，属于不那么急的。比如告知下一站到站还需多长时间（测算 TA 值提前量，让人提前做好准备），播报一下空气质量（无线链路质量），点一首歌送给某人（短消息）。

第二类称为 FACCH，是快速的、紧急的服务。比如说本火车抛锚了（无线链路接收电平太低，TA 值超限，或者通信质量不行了），请赶快换乘另一辆列车（切换）。

（1）慢速随路控制信道（SACCH，Slow Associated Control CHannel）

SACCH 与一个 TCH 或一个 SDCCH 相关，在上行方向，传递 MS 接收到的当前服务小区以及相邻小区的信号强度的测试报告，以及链路质量的报告，这对 MS 的切换而言相当重要，BSC 要根据这些信息来判断把它切换到哪个小区上去。

在下行方向，它传递功率控制和定时信息。

（2）快速随路控制信道（FACCH，Fast Associated Control CHannel）

之所以要引入快速随路控制信道，就是因为慢速随路控制信道实在是太慢了，能传递的信息量也太少了。到底传递的信息量有多少呢？速率有多慢呢？

我们在 3.2.1 节的信道编码中已经介绍过 SACCH 的编码了，一个 LAPDm 帧是 23Byte，合 184bit，SACCH 的有用信息也是 184bit。但这只是原始信息，我们还要经过

信道编码，经过信道编码后就成了 456bit。每个突发脉冲可以传递 57×2=114bit。那么 456bit 就需要 4 个突发脉冲才能传完。每 26 帧中共有 25 个 TCH 帧和 1 个 SACCH 帧，那么要传完 4 个 SACCH 帧一共需要的时间是 4×26×4.615ms=480ms。480ms 才能传完 184bit 的有效信息，那么 1s 可以传递多少比特的有效信息呢？不难算出来，184bit×1s/480ms=383bit。

这样我们就可以得知，SACCH 的速率为 383bit/s，要传完一个完整的信息，延迟达到 480ms。对于切换这种需要快速处理的信息，是完全派不上用场了。

如果要快，就不能等语音信号传完到空闲的时候再传信令。我们只能“偷帧”，借用 TCH 的帧来传递信息。

图 5.16 所示的两个 Flag 位，就是偷帧位，我们将前后两个 Flag 位都设为 1，那么该 TCH 帧就整个变成 FACCH 帧了。如果只将 1 个 Flag 位设为 1，另一个还是 0 的话，就只有一半的帧归 FACCH 所用。

尾比特 3bit	加密比特 57bit	Flag 1bit	训练序列 26bit	Flag 1bit	加密比特 57bit	尾比特 3bit	保护间隔 8.25bit

图 5.16　普通突发脉冲序列

5.3 复帧的应用

复帧的应用对于很多人而言是个难题，其难点倒不在 26 帧的 TCH 复帧，一个 26 帧的 TCH 复帧除了 24 个 TCH 帧外，就只有一个 SACCH 帧以及一个空闲帧，相对而言比较简单。而 51 帧的控制信道复帧就相当复杂了，它可能包含 FCCH 帧、SCH 帧、BCCH 帧、CCCH 帧、SDCCH 帧、SACCH 帧以及空闲帧，看得人头晕眼花，想要一下理清楚并不容易。

我们知道，每小区有若干块载频，定义为 C0～C*n*，每载频有 8 个时隙，定义为 TS0～TS8。除了 C0 号载频的 TS0 是控制信道外，其余的通通为 TCH（这种说法不太严谨，C0 载频的 1 号时隙可能为 SDCCH）。鉴于 TCH 比较简单，我们就把它抛开在一边不管，只研究 C0 载频的 TS0 时隙，也就是控制信道究竟是如何应用的。

从图 5.17 中我们可以看出，这 51 帧的由来还是比较简单的，就是由 51 个 TDMA 帧的 0 号时隙组成的。现在的问题是，对于这个 51 帧的复帧，它的这些信道，譬如 FCCH 帧、SCH 帧、BCCH 帧、CCCH 帧、SDCCH 帧、SACCH 帧，究竟如何组合成复帧呢？



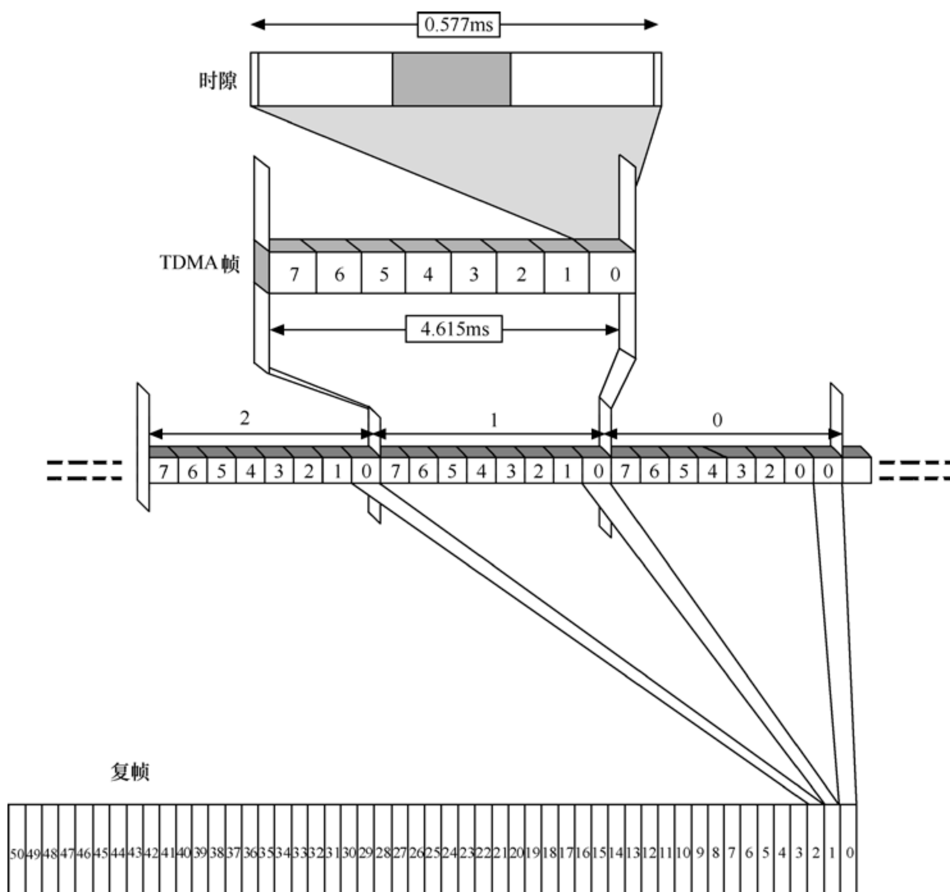


图 5.17　51 帧控制信道的映射

有两种比较常见的信道组合，我们来看一下它们的上下行都是如何组成的：

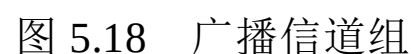
（1）广播信道组（用于 C0 载频的 0 号时隙）——BCCH+CCCH；

（2）专用信道组（通常用于 C0 载频的 1 号时隙）——SDCCH8+SACCH8。

由图 5.18 可见，在上行方向，所有的时隙 0 都分配给了 RACH，因为 RACH 是广播信道和公共信道中唯一工作在上行方向的。

还可以看到，BCCH 其实是个小容量的信道，仅比 SACCH 强一点，51 帧的复帧，只有 4 帧是留给 BCCH 的。BCCH 和 SACCH 同是传递 184bit 的有效信息（经过信道编码后为 456bit）。SACCH 需要 26×4=104 帧，而 BCCH 需要 51 帧，那么 BCCH 的速率就是（184bit×1s）/（51×4.615ms）=782bit/s。差不多是话务信道上的 SACCH 的 383bit/s 速率的两倍。

R=RACH
B=BCCH
F=FCCH
S=SCH
C=CCCH
I= 空闲


图 5.18　广播信道组

在下行方向上，共有 9 个 CCCH 块，我们知道，CCCH 上行方向只有 RACH，下行方向只有 PCH 和 AGCH。至于 CBCH，占用的其实是专用控制信道（如 SACCH 和 SDCCH），只不过因为它是广播形式发送出去的，所以我们把它放在通用控制信道里了。



1. 通用控制信道的参数

我们下面讲一下 GSM 网络中常见的几个关于通用控制信道的参数。

（1）通用信道配置（CCCH CONF）

这个参数用来指示配置了几个 CCCH 消息块，图 5.18 举例是配置了 9 个块。其中 4 个帧为 1 个块，这好理解，因为 184bit 的 CCCH 信息经过信道编码后是 456bit。1 个帧能容纳 114bit（57bit×2=114bit），那么要 4 个帧才能组成一个消息块完成 184bit 的信息。对这一块内容不熟悉的请看图 5.19 所示的普通突发脉冲序列组成图，并再翻看一下 3.2.1 节。

尾比特 3bit	加密比特 57bit	Flag 1bit	训练序列 26bit	Flag 1bit	加密比特 57bit	尾比特 3bit	保护间隔 8.25bit

图 5.19　普通突发脉冲序列

（2）接入准许保留数（BS AG BLKS RES）

这个名字有点拗口，其实其作用就是告诉我们这 9 个 CCCH 块里面有多少个是留给 AGCH（接入允许）用的，所以称之为接入允许保留数。

除去接入允许占用的块数，剩下的就都归 PCH 了。这样就得出了下面的公式：PCH 块数目=CCCH CONF（CCCH 信道配置数）−BS AG BLKS RES（AGCH 占用的数目）。

（3）寻呼信道复帧数（BS PA MFRMS）

这个参数是做什么用的呢？如果说 BS AG BLKS RES 定义了 51 帧的 BCCH 复帧有多少个 PCH 的话，那么 BS PA MFRMS 就定义了总共有多少个子信道。因此有

PCH 子信道数目=PCH 块数目×BS PA MFRMS

那么 PCH 子信道又有什么含义呢？

根据 GSM 规范，每个移动用户（即对应每个 IMSI）都属于一个寻呼组，在每个小区中，每个寻呼组都对应于一个寻呼子信道。在实际网络中，移动台只收听它所属的寻呼子信道的内容而忽略其他寻呼子信道的内容，甚至在其他寻呼子信道期间关闭某些硬件设备的电源以节约移动台的功率开销（参见 3.3.3 节）。

举一个例子：假如我现在有 36 个用户需要寻呼，假设现在 PCH 块数为 3，把 BS PA MFRMS 设为 2，那么就有 3×2=6 组寻呼子信道。48 个用户就分布到这 6 组寻呼子信道中进行寻呼，相对来说这个寻呼的密度就要大一点。如果我们把 BS PA MFRMS 的值设为 4，那么就有 3×4=12 组寻呼子信道。相对来说，每个子信道的压力就要小一点，但同时随着 BS PA MFRMS 值的增加，时延也增加了，我们需要在两者之间有个折中。

下面再来看看专用信道组——SDCCH8+SACCH8 的组成，如图 5.20 所示。该种信道一般用于 0 号载频的 1 号时隙，紧跟在 BCCH 时隙之后，但其实是可以配置在任何时隙的。

图 5.20 所示是一个 8 个 SDCCH 的 51 帧复帧结构，要完成整个序列需要用到 2 个 51 帧复帧，逻辑上可把它看作一个 102 帧的复帧结构。

图中的 SACCH 和 SDCCH 是一一对应的，如 D0 对应 A0、D1 对应 A1、D2 对应 A2、D3 对应 A3、D4 对应 A4、D5 对应 A5、D6 对应 A6、D7 对应 A7。

图 5.20 SDCCH/SACCH 复帧结构



在这里，上下行是错开 3 个时隙的，以便于移动台有足够的时间处理接收到的信息和作出响应。

2. SCH 的测量

前面说过，将业务信道设置成 26 帧，控制信道设置成 51 帧，并且两者之间连公约数都没有，是有其深意的。26 帧业务信道中设置了一个空闲帧，也不是吃干饭的。它们都有其目的，到底有何用意呢？

我们知道，手机在通话的时候（占用 TCH 时隙）还要对周围 6 个信号最强的邻小区的接收电平进行测量，以用于切换。为了防止测到了非相邻小区的同频频率（非相邻小区你要切换的时候是切换不过去的，但是如果其接收电平很强，很容易被你的手机测试到），那么就需要读这 6 个邻小区的 BSIC 号，以免搞错。所以，同频同 BSIC 是要绝对避免的，否则会造成掉话！

什么时候来读 BSIC 号呢?手机占用 TCH 的时候是没有空来读周围邻小区的 BSIC 的，毕竟那要花时间，就只有靠空闲（Idle）帧了。问题是，当且仅当你的手机在空闲帧，周围的 BTS 在 SCH 帧上时你才有机会读取它。现在我们就看看，将业务信道设置成 26 帧，控制信道设置成 52 帧，在原有的 51 帧的尾部加一个空闲帧，会造成什么后果。

我们在图 5.21 中画出了控制信道和业务信道复帧从 0 号帧到 103 号帧的对应关系。可以看出，假设控制信道复帧数为 52，恰好为 TCH 复帧数的两倍。问题就出来了，那就是 26 帧的业务信道复帧和 52 帧的控制信道复帧每帧的一一对应关系始终不会变化！

我们发现，在 0～51 号帧时，业务信道的两个空闲帧分别听取的是别的 BTS 的通用控制信道（CCCH）和 Idle 帧的内容。在 52～103 号帧的同时，听取的同样是这两个位置的内容。不难看出，在 104～155 号帧、156～207 号帧……乃至后面的内容，业务信道空闲帧听取的控制信道复帧的内容还会是 CCCH 和 Idle。

也就是说，占用业务复帧的 MS 根本无法听取到另外一个邻小区 BTS 发送的 FCCH 帧和 SCH 帧，也就根本无法完成锁频和读取 BSIC。不能对邻小区完成锁频和读取 BSIC 的话，也就无法将这些信息上报给 BSC，BSC 不知道这些信息的话，切换也就成了一场空谈。

或许有人会不同意我的意见，因为小区之间的起始帧号一般不会是相同的，也就是说，很少出现当前通话小区的 TCH 的 0 号 TDMA 帧和邻小区通用控制信道的 0 号 TDMA 帧刚好对应的情况。如果有一个偏差，比如说控制信道现在在 0 号 TDMA 帧，而 TCH 现在在 25 号帧（第 26 帧，即空闲帧），那么当前的 MS 不就可以听取到邻小区的 FCCH

了吗？

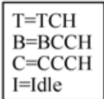


图 5.21　假设控制信道复帧结构为 52 帧

话的确是如此，不过我们可以看看图 5.22，这种情况下并没有对刚才的局面有所

改观。TCH 和通用控制信道的对应关系还是固定不变的，不过是由刚才的听取 Idle 帧和 CCCH 帧变成了听取 FCCH 帧和 CCCH 帧，你依然无法听到邻小区的 SCH 帧和 BCCH 帧，依然无法完成和邻小区的同步，也不知道邻小区的相关信息，当然也谈不上切换。

图 5.22　52 帧的控制信道与 26 帧的业务信道



由图 5.21 和图 5.22 可以得出这样一个结论，将控制信道设为 51 帧和将业务信道设置成 26 帧，其目的是为了让业务信道的复帧和控制信道的复帧之间的时间对应关系不断改变，这样使 MS 能接收周围小区的 FCCH、SCH 和 BCCH 信息，这对手机通话过程中的切换很重要。

如果业务信道和控制信道复帧的帧数一个正好是另一个的整数倍的话，那么控制信道和业务信道帧在时间上的对应关系就永远不会变化。而实际上，这种两种复帧之间不停变化的对应关系是非常重要的，一个 MS 需要监视和报告相邻小区的 RSSI 值，它就必须“看到”其他小区的 BCCH。手机若无法利用空闲帧有效获取邻小区的相关信息，那么切换也就无法进行了。

我们在前面扯了一大堆，反复强调了 51 帧控制信道复帧和 26 帧业务信道复帧之间在时间上的对应关系不断变化的重要性。那么，SCH 的测量到底是如何完成的，下面用图 5.23 进行解释说明。

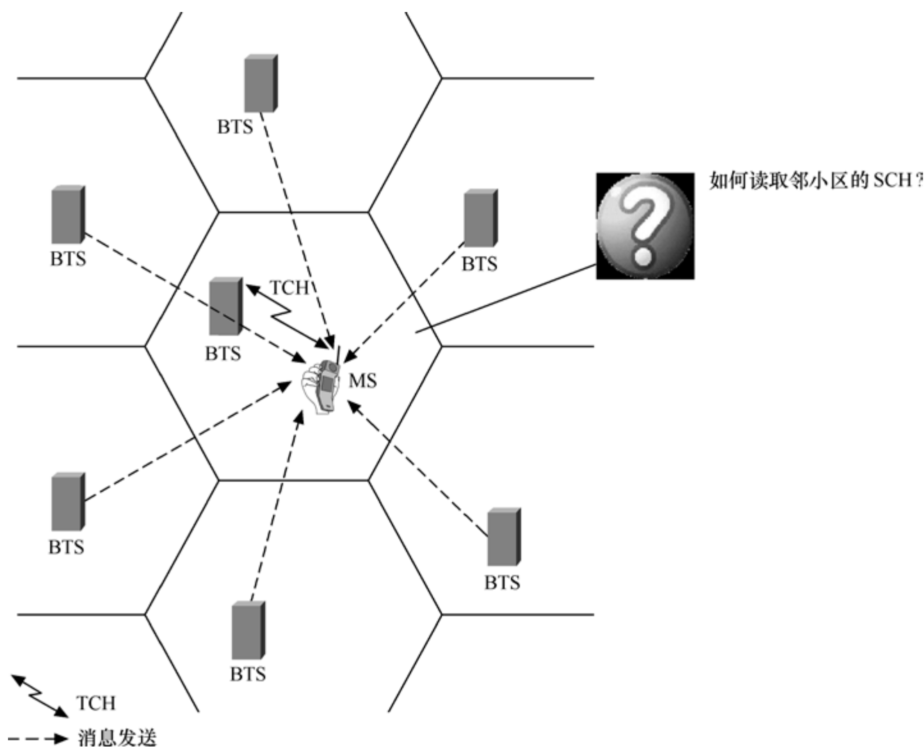


图 5.23　如何读取邻小区的 SCH 过程

我们知道，移动台在通话时，只有通过 TCH 信道 26 复帧的空闲帧才有时间去对 SCH 进行解码。除了读取邻区的 BSIC 信息和 TDMA 帧号信息之外，移动台还需要测量本小



区的接收电平和邻小区的接收电平，这些工作都是什么时候完成的呢？

① 移动台在"接收结束—发送开始"这段时间内测量本小区的接收电平和信号质量；这里大约有 3 个时隙的时间（注：之所以说大约 3 个时隙是因为我们在 3.2.4 节中说过，手机发送的时候需要考虑一个时间提前量 TA，所以实际上不足 3 个时隙）。

② 移动台在"发送结束—接收开始"这段时间内不仅可以测量本小区的接收电平和信号质量，还可以测量邻小区的接收电平。

③ 移动台在空闲帧的时候解码邻小区的 SCH，读取 BSIC 和 TDMA 帧号，问题是 SCH 帧每隔 10 个帧才出现一次，你未必有那么好的运气第一次就能撞上，但是你运气再背，10 次总能撞上吧！我们用图 5.24 演示一下这种测量方法，称为滑动测量，在图中是滑动了 4 次然后测到了 SCH。

我们首先通过图例来说明以上 3 项工作，图中 5.25 中所示的 MS 在第 2 时隙上收取 BTS 的信息。我们在图中用①来标注工作①，用②来标注工作②，用③来标注工作③。

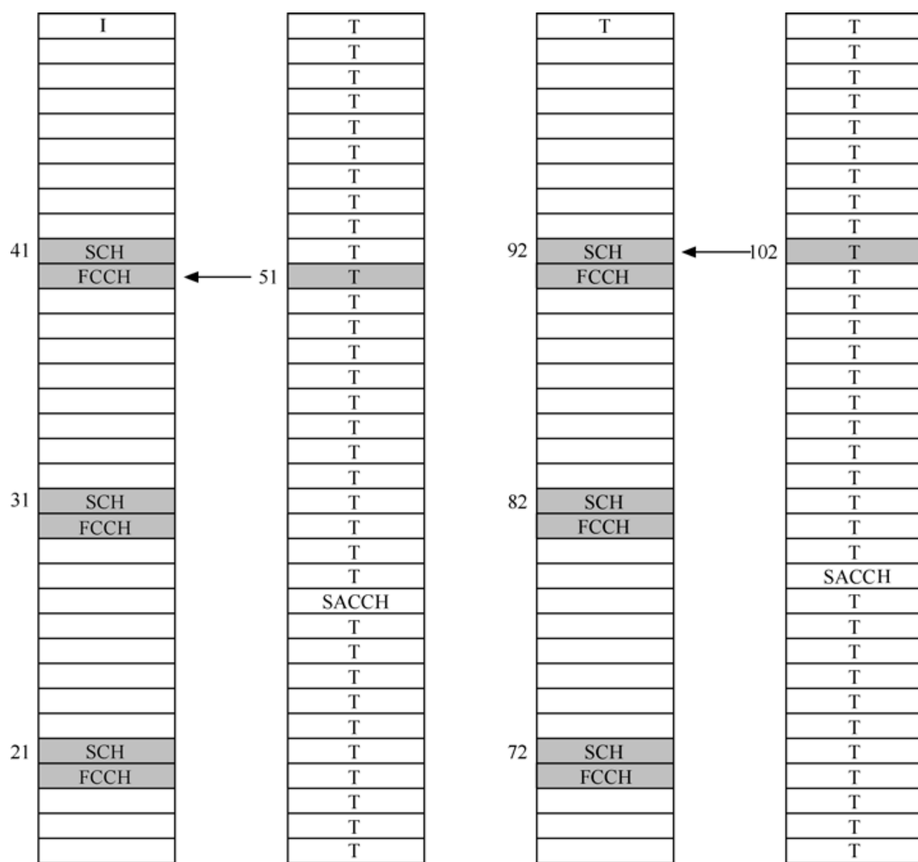


图 5.24　SCH 的滑动测量（4 次滑动测量出 SCH）

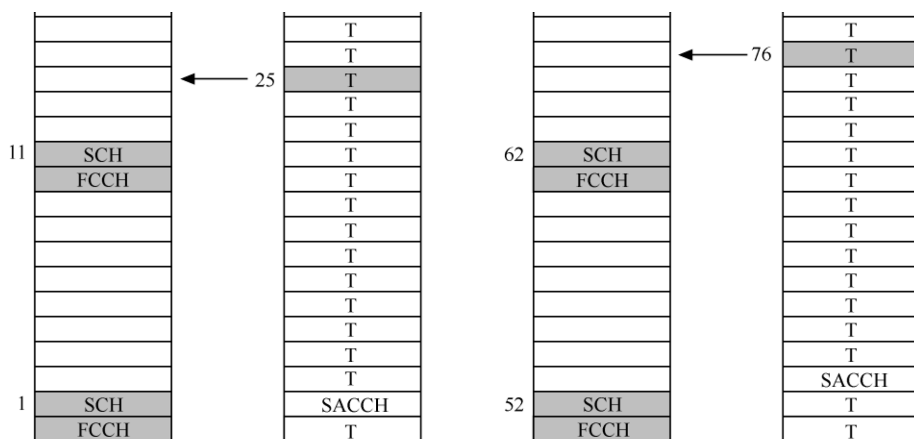


图 5.24　SCH 的滑动测量（4 次滑动测量出 SCH）（续）

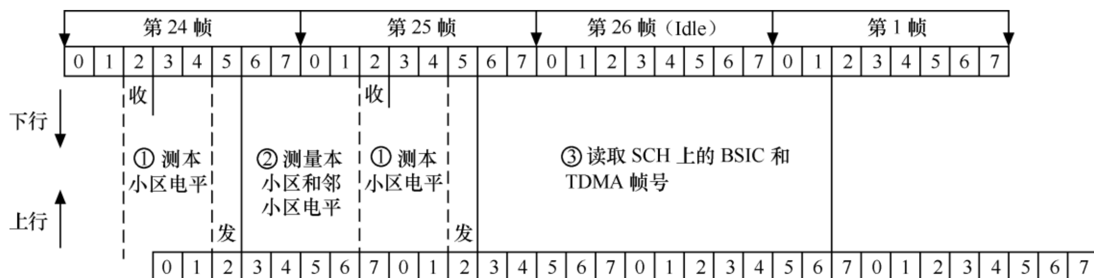
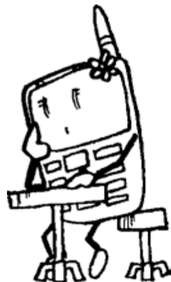


图 5.25　测量电平值和读取 SCH

第 6 章

Chapter 6



无线通信的特质——也谈 GSM 第三层协议

第 6 章和第 7 章的内容是为第 8 章打基础的，如果不对 GSM 的第三层协议以及七号信令的内容有所了解，直接去进行信令流程的学习恐怕是很困难的。在本章所说的 GSM 第三层协议包含无线资源管理（RRM，Radio Resource Management）、移动性管理（MM，Mobility Management）和接续管理（CM，Connection Management）。

6.1 固定通信与移动通信的区别

应当说移动通信在很多方面都比固定通信要复杂得多。移动通信有其固有的特质，比如说通信位置不固定，信道资源极其有限（空中接口的频谱资源），需要进行鉴权和加密以防止窃听（电磁波在空中四散传播，谁都能接收到）。这都给无线通信带来了极大的困扰，为了让用户有完美的通信体验，我们需要设计一系列应对措施，这就是 RRM、MM 和 CM 的由来。

无线通信与有线通信的主要差异在于接续资源的管理。在有线网中用户终端和系统之间的通信介质总是存在的，电路总是预留着的，当客户需要进行一个呼叫时，可以立刻建立电路连接。而对于 GSM 而言，空中接口的频谱是非常有限的，显然不可能这么奢侈地为每个用户预留一条信道，为了提高系统资源的利用效率，就必须资源共享，路径必须按需分配，无线接口上的信道仅仅在 MS 需要和通话期间提供，通信结束时进行释放，信道的分配和释放都受到系统的控制。

另外，在有线固定通信网中，信令信道总是存在的，电话线在，故信令链路在。而

对于 GSM 网络而言，对于一个空闲模式下的 MS（即没有分配信道，没有建立一条专用信道情况下的终端），其信令能力被限制到了最小，仅够维持网络对 MS 的跟踪（位置更新），以及 MS 对小区的识别和网络情况的一些了解（BCCH 广播系统消息）。

除了信道的分配有差别之外，移动通信相对固定通信还有一个特别的概念，那就是切换。在有线通信时，用户的位置是基本不变的，其通话所用的接口和电路都不会改变。而移动通信则大不相同，用户的位置在通话过程中不断变化，完全可能穿越多个基站的覆盖区域，要保持通信不中断，就必须进行切换，即把 MS 和网络的连接从一个小区转移到另一个小区。除了保持通信不中断以外，信道切换的一个重要功能也是通过把通话转移到信号质量更好的小区来保证通话的质量。

为了实现这些功能，需要有复杂的信息交换和管理过程，这些信息交换和管理称之为信令。我们上面说过，GSM 层 3 信令可以分为 3 个实体：无线资源管理（RRM）、移动性管理（MM）、接续管理（CM）。RRM 的职能在于管理无线接口，包括信道的配置、传输的模式、上下行电平及通信质量的测量、切换的操作等内容，其目的在于建立一条点对点的链路，并负责这条链路的维护和控制；MM 是建立在 RRM 之上用于处理移动性和安全保密性的功能组；CM 位于上述两组之上，用于完成点对点通信的建立和释放。

RRM 和 CM 看起来都是点对点的管理，其实质内容却大不相同，我们可以用通俗一点的比喻来形容它们的区别：RRM 就一公路局的，怎样把公路从长沙修到武汉并保证这条公路不出问题是它们要干的活，它们都时刻监控公路的质量；而 CM 是搞物流的，怎样在公路上实现货物的调度运输，交换转运，从而实现货物点对点的传送是它们的专业，可以看出 CM 是建立在 RRM 之上的，公路都没有，谈何物流！

6.2 频率贵如黄金，吾等自应珍惜——无线资源管理（RRM）

又是老调重弹了，空中接口的资源非常宝贵和有限，我们必须要进行有效管理，资源管理的很大一部分工作就交给 RRM。RRM 的主要作用是协调 MS 与 MSC 之间的传输，对每个申请通信的 MS，建立起一条自 MS 至 MSC 的传输路径和信令路径。

6.2.1 好的开始是成功的一半——RRM 的初始化阶段

MS 有两种不同的工作模式：空闲模式和专用模式，这两个概念在信令流程里用得非常之多。所谓空闲模式，指的是移动台没有和系统建立连接时的状态；所谓专用模式，指的是 MS 已经工作在一条激活了的全双工信道上的状态。



在空闲模式下，MS 将进行以下 4 个事项：网络选择、小区选择、小区重选、位置更新。

在专用模式下，MS 将出现寻呼、立即指配、鉴权加密、主叫、被叫、短消息、切换、信道模式改变、链路释放、呼叫重建、功率控制等事件。

这些事件的信令流程我们会在第 8 章里进行详细叙述，在这里，我们先关注 GSM 系统如何对无线资源进行管理。

从空闲模式向专用模式转换的过程就进入了 RRM 初始化阶段，称之为接入（Access）。接入过程可以有两种方式：一种是 MS 发起（MS 主叫或者位置更新）；另一种由网络侧发起（MS 被叫）。要和被叫用户进行通信先得让被叫接入网络，如果被叫现在的状态正常（没有关机或不在服务区），那么就可以通过寻呼找到被叫，因为 MS 在空闲模式下总是在收听某个寻呼信道（PCH 信道）的寻呼信息。当它听到是在寻呼自己的时候，它就发起一个连接，要求接入网络。

这就好比上课回答问题一样，你可以主动举手回答问题（主叫要求接入），也可以等老师点你的名（PCH 信道寻呼）然后回答问题。MS 接入与课堂回答问题不同的一点就是老师是点对点通信的，他点了你的名你直接站起来回答问题就可以了，不用再举手；而 MS 接入则不同，虽然网络已经对你做了 PCH 寻呼要求你接入网络（点名），但是你接入网络前还得申请信道（举手），因为 BTS 对 MS 而言是点对多点的，它同时要处理 N 多 MS 的通信需求，虽然点了你的名，但有没有资源另说，所以 MS 即使作为被叫接入网络还是得先申请信道，不举手就乱发言课堂就乱了套了。

MS 的接入方式如下：MS 通过在随机接入信道（RACH）上发送一个消息要求接入网络，网络通过接入许可信道（AGCH）发送立即指配（Immediate Assignment）作为响应，为该 MS 指定一条专用信道。RACH 信道工作在 0 号时隙通用控制信道的上行方向，属于众多 MS 共享的资源。由于每个 MS 的接入请求是随机的，所以完全可能出现信号碰撞的现象，如何解决这个问题呢？RACH 借鉴了局域网的 ALOHA 协议，局域网那 HUB 就是多用户共享型的，遭遇这样的问题多了，早就有成熟的解决方案，我们会在后面详加阐述。

寻呼过程（Paging）是网络侧用来触发 MS 进行 RR 连接的方式。由于 MS 用户的移动性，我们需要首先确定被叫 MS 的位置，总不能从南京到北京的来个全国的寻人启事。确定 MS 位置的过程与 MM 管理密切相关。这个过程是这样的，首先，MSC 负责向 BSC 提供被叫用户的 IMSI 号，BSC 会组织寻呼要覆盖的小区表（通常情况下，同一个 BSC 下的所有小区属于同一个寻呼区，这就意味着是对该 BSC 下所有小区进行寻呼）；其次，BSC 要编组和安排寻呼消息的发送及重复次数，确定被叫的 IMSI 号与寻呼子信道之间的关系，然后选择合适的寻呼信道发送消息。



寻呼信道是下行公共信道控制的一部分，属于某个用户的寻呼消息总是在同一寻呼子信道上发送。这样可以减少 MS 在空闲状态下需要接收的信息量，从而降低手机的功耗。

6.2.2 多宽的车走多宽的路——RR 的传输管理

对于很多从事通信工作的人来说，这个标题有点令人困惑。因为我们通常意义上默认传输这个词就用于“SDH—SDH”之间的通信设备和光缆了。本文的传输不是这个意思，凡是把信号从一个地方送到另一个地方都可以称之为传输，BTS 给 MS 发送信号可以称为传输，MSC 给 BSC 发送信号也可以称为传输，这里说的传输是广义的传输。

之所以有这项工作主要原因还是因为无线信道模式有多种，比如 TCH/F、TCH/H、TCH/8（即 SDCCH）等。GSM 是很抠门的，什么都精打细算，你如果只是发发短信，传传信令，那么就给你分配一条 SDCCH 信道好了。啥，你想占用一条 TCH/F，这个是要 Money 的，连想都别想。这样一来有一种人就冤枉了，他想打电话，然后通过 RACH 申请接入网络，网络侧通过 AGCH 信道给他分配了一条 SDCCH 信道，传传信令先，鉴个权，验明正身什么的。现在权也鉴了，BTS 到 BSC 乃至 MSC 的链路也分配好了，他还是占着 SDCCH，可是 SDCCH 信道容量小，玩不了话音啊。没办法啊，资源宝贵啊，还没验证你是不是合法用户，链路也没调通，哪能让你占着宝贵的 TCH 信道呢，那都是爱尔兰，都是收入啊！既然现在一切就绪，那我就派一名大将（RR 传输管理）出马，把你的信道模式修改过来，让你用 TCH 信道好了。

信道就是资源，资源就是金钱，搞企业管理的，样样都得精打细算，搞不好哪天现金流出现问题就得破产，所以这个资源一般不是谁都能分配的，得老总（MSC）亲自出马。然而，在 RR 的初始接入阶段，也就是 RACH 接入和立即指配阶段，MSC 是不明确 MS 所需的模式的，这个时候就由 BSC 选择信道，信道可以是任何类型的，但通常是分配 TCH/8（SDCCH），仅做信令交换用。这就好比老总（MSC）不知道客户想做的业务到底有多大，就先授权部门经理（BSC）出面，给他分配资源的权力，让他先试试水深水浅。权是放了，可是老板的第三只眼盯着呢，部门经理（BSC）哪敢放肆，就分配给客户（MS）一条小小的 SDCCH 业务，咱先交流交流，鉴别鉴别，等明确了再汇报给老板，到时候再搞个业务经理（RR 传输管理）给你改信道也行。

在这之后，根据用户业务的需求，MSC 选择适当的模式，并为其建立相应的 RR 路径，包括 MSC 与 BSC 之间的有线路径。尽管 MSC 在模式的选择权上有决定权，但实际信道的选择以及不同设备之间的协调还是由 BSC 来具体完成的，包括 BTS 与 MS 之间无线路径的决定（哪块载频，哪个时隙）。这就好比老板与部门经理的分工，老板负责宏观的调度，具体的分工协调都是部门经理去做，部门经理这一层要求的就是执行力，“把信送给加西亚”嘛，你看信都给你了，还不去送给加西亚？



这上面的传输管理就包括两方面的内容：其一是 MSC 必须在 RRM 期间随时通知传输模式改变的要求；其二是 BSC 要能组织 MS 和 BTS 来满足 MSC 的需求。

这些链路是这样组织的：在 Um 口，BTS 载频—MS 的无线链路是 BSC 分配的；在 Abis 口，BTS 载频—BSC 的链路本来就是一一对应的，不需要进行分配；在 A 接口，MSC 把电路分配给相应的 RR 连接，并以信令的方式告知 BSC，BSC 通过交换功能（我们在 4.6 节提过 BSC 的 TDM 交换功能）把指定的无线路径（从 MS 到 BTS 到 BSC）与这条 A 接口电路相连（CIC 的分配）。

除了无线信道的修改，传输管理还有两大任务：一是加密模式的管理，二是非连续发射模式（DTX）的管理。

RR 连接总是开始于无加密的信令方式，是否加密由 MSC 决定，由于第 8 章中还将讨论这方面的内容，在此不再详加叙述。

非连续发射的目的是把无线路径上的功率发送减到最小，以便节省 MS 的电量和减小相互间的干扰。我们在 3.3.2 中就这个问题有过详细的讨论，就不在这里重复了。

6.2.3　跳槽还需细思量——切换的目的及依据

切换就相当于职场中的“跳槽”，切换是从一个小区换到另一个小区，跳槽是从一个企业跳到另一个企业。跳槽需瞻前顾后，仔细考虑和衡量各方面的因素，切换又怎能不细加思量，综合考虑各个小区的资源情况和链路质量情况。

切换也是 RRM 中非常重要的功能，切换在蜂窝通信中的重要是毋庸置疑的了，这简直就是移动通信的基础。只要你“移动”，就可能来到别的小区，就可能产生切换；即使你不“移动”，空中无线链路的情况也一刻不停地在发生变化，你目前这条通话的链路完全可能变得质量很差，从而被迫切换到别的小区。

切换的目的有以下几种：一是保证当通话中的 MS 超出当前小区覆盖范围时，不至于产生掉话；二是当通话中出现强干扰时，能够换到别的小区从而避免干扰；三是 MS 当前小区出现拥塞时，MS 能够切换到相邻小区，从而避免拥塞。

根据切换的目的可以衍生出多种切换判决的方法。

一是根据通信质量来进行判决，其依据是上下行的接收电平和误码率，因为误码率和接收电平息息相关，所以两个指标总是放在一起。接收电平和误码率都是要进行测量然后上报给 BSC 的，MS 和 BTS 都需要有规律地测量上下行的传输质量和接收电平。其中 MS 测量电平和传输质量的过程我们在 5.3 节中有过详细的阐述，测量完之后 MS 通过 SACCH 信道以每秒两次的频率上报给 BTS 再转给 BSC。

二是根据 TA（Time Advance，时间提前量）值来进行判决，有关 TA 值的内容我们在 3.2.4 节中提过。GSM 是个 TDMA 系统，定时的精准性是很重要的，时延太大是不受

欢迎的，通常系统都可以设置一个 TA 门限，超过该门限就要进行切换。

三是拥塞引发的切换，需要根据每个 BTS 的当前负载情况进行判决。BTS 是不知道别的 BTS 的负载情况的，这个值只有 MSC 和 BSC 知道。这个过程是要求在给定的小区内，由于话务量的原因，命令一部分 MS 切换。

GSM 切换算法和目标小区选择方法在 GSM 规范里只给出了建议，而非强制性的，所以各个厂家也往往有自己的实现方法。切换的信令流程我们会放到第 8 章里详细讲。

6.2.4　炒炒冷饭——功率的控制与时间提前量

功率控制和时间提前量也是 RRM 的内容，它们有一个共同的目的就是为了改善频谱资源使用效率及延长手机的电池使用寿命。功率控制的内容和时间提前量的内容分别位于本书的 3.3.1 节和 3.2.4 节，就不在这里加以重复了。

6.2.5　要唱戏还得先搭台——小区信道的配置与分配

上面 RACH、PCH、信道模式修改、切换讲了一大堆，各色人物轮番上台唱戏，不可谓不丰富。不过且慢，要唱戏得先搭台吧，我台都没搭唱什么戏呢。对于 RRM，如果上面的内容算是唱戏，那什么算是搭台呢——那就是信道的配置了。有面包才有玫瑰，精神层面的愉悦建立在物质的基础上，载频和信道都没配，所谓的 RR，即 Radio Resource 根本就没有，谈何 RRM 啊。

如果说上面所说的都是在已经配置好的信道上进行的 RRM 工作，那么下面要讨论的内容是小区信道的配置与分配原则。这也是无线资源，也属于 RRM 的内容。

1．小区信道的配置

小区信道的配置是一个相对长期的管理，一个典型的小区配置包括一系列的公共信道用于支持空闲模式 MS 和 MS 的初始接入（如 BCCH、PCH、RACH 和 AGCH），还有一部分是话务信道用于支持通话和通话中的控制与监测（如 TCH、SACCH 和 SDCCH）。

小区配置的另一方面是动态修改业务信道（TCH）以满足业务需求。例如当 SDCCH 信道不够的时候，可以将一个 TCH/F 用作 SDCCH/8，GPRS 的信道调整也与此类似。

2．专用信道和业务信道的分配

我们在 6.2.2 节中已经讨论过这个问题。RR 接续期及之后信道的分配也属于 RRM 的内容，专用信道和控制信道可以根据 MS 的不同需求分给它，主要有 3 种情况。

（1）初始信道分配：RACH 初始接入时分配，一般分配 SDCCH。

（2）后继分配：如当前使用的信道类型和所需要的信道类型不一致时，进行无线信



道模式的修改。6.2.2 节中有所描述，比如初始分配的是 SDCCH 信道，有通话需要的时候可以修改为 TCH/F 信道。

（3）切换分配：当 MS 越区或者质量变坏或者 TA 超限时进行切换处理，切换处理时也需要分配信道。

信道的分配共有两项工作要做：一是信道的选择；二是激活所选择的信道。BSC 负责信道的选择和激活 BTS 上的信道。激活一条分配的信道，需要 BSC 预先知道每个空闲信道的连接情况，这其中很多因素是难以确定的，但是上行的干扰电平却是确定的，因为 BTS 总是周期性地对所有空闲信道上的干扰电平进行测量，并把结果汇报给 BSC 以供参考。

对于 TCH 信道的分配，又有 3 种情况。

（1）超前分配：当 MS 要求连接时，马上分配 TCH/F，这很少见，一般用于传递大信息量的时候。

（2）提前分配方式：当 MS 要求连接时，先分配 SDCCH，然后尽可能早地分配 TCH/F，这是最常见的方式。

（3）滞后分配方式：当 MS 要求连接时，先分配 SDCCH，尽可能晚地分配 TCH/F，直到被叫应答后再分配 TCH。这种方式资源利用效率最高，但随之带来的延时也是一个不得不考虑的问题。

3. 无线信道的描述

信道配置完了，还有一项重要的工作就是把配置消息告诉周围的 MS。这个工作并不轻松，信道的特性可以由时间和频率两方面构成。在时域上，根据不同的信道类型和时间偏移量，可以分为 8 类 TCH/F 信道和 68 类 TCH/8 信道，总计 76 类信道；如果包括半速率情况则可多达 92 类。信道的组成比较复杂，我们不在这里展开叙述，详见《GSM 900M 无线接口物理层规范》。对于这类信道的识别需要占用 1 字节（Byte）的编码。

在频域上，GSM900 频段有 124 组频点，而在 DCS1800 频段还有 374 组频点。加上可能的扩展频段，总共用 10 位编码表示频点识别。

因此 18 个比特就可以唯一地对应一个信道。

描述跳频的话情况还要复杂一点。在 GSM 系统中，每个小区所使用的载频的集合用“小区分配（CA）”来表示，记为{R_0，R_1，…，R_{N-1}}。为了描述一个跳频信道我们引入频率表的概念，在 GSM 规范中称之为移动分配（Mobile Allocation，MA）表，MA 是 CA 的一个子集；另外还要用到两个参数来计算跳频序列，这两个参数就是移动分配索引偏移量（MAIO）以及跳频序列号（HSN）。

在每次通信过程中，空中接口的载频号都是集合 MA 中的一个频率，称之为“移动分配索引（Mobile Allocation Index，MAI）”，之所以说成是索引，因为它并不表示实际

的绝对频点号，而是表示频点号在 MA 表中的相对位置。打个比方，如果说 MA 表包含了以下频点{4，16，22，25，27，31}，那么 MAI 索引号为 4 的就表示了 25 号频点。

我们知道了 MAI，那么 MAIO 又是什么意思呢？MAIO 称为移动分配索引偏移量（Mobile Allocation Index Offset），MAIO 的目的是给不同的载频予以不同的初始偏移量，免得它们争抢同一个频点。

HSN 的作用是规定跳频序列，我们刚刚举例说的 MA 表{4，16，22，25，27，31}只不过是定义了可以采用的跳频的频点。到底是“4—16—22—25—27—31”还是“31—27—25—22—16—4”或者采用其他的跳频序列这不归 MA 表管，归 HSN 管。

同一个小区应当采用相同的 HSN，不同的 MAIO。

不同的相邻小区应当采用不同的 HSN。

6.2.6 念念这本经——RRM 协议

家家有本难念的经，对于 GSM 而言，RRM 这本经大概最难念了，内容又多又复杂，在本节中，我们就打算对 RRM 协议的内容都理一理。

RRM 的主要功能都在 BSC 侧，MSC 和 BTS 也要承担一部分 RRM 的工作，BTS 要上报各种测量结果供 BSC 和 MSC 对无线链路进行判断。而 MSC 参与的就更多了，从信道的分配到信道模式的修改，从加密模式的下发到给 MS 的寻呼，几乎都有它老人家的参与。

MSC、BSC、BTS 都扯上了，下面来看看 RRM 具体包括哪些方面。

（1）初始过程：随机接入和信道分配。

（2）寻呼过程的管理。

（3）传输模式与加密模式管理过程。

（4）切换判决与处理。

（5）呼叫重建。

（6）RR 连接释放。

（7）负载管理过程。

（8）SACCH 管理过程。

（9）广播消息（系统消息）。

这些内容与第 8 章的信令流程都是密不可分的，是学习信令流程的基础。本节的内容和第 8 章不可避免地会有一些重复，把 RRM 这部分从信令流程里单独列出来讨论是为了加深对它的理解，同时尽量降低第 8 章的难度。

1．初始过程——随机接入和信道分配

随机接入 RACH 和信道分配 AGCH 我们在上面已经粗略地提了一下，引发随机接



入的原因可能有以下 3 种。

（1）执行小区位置更新；

（2）响应寻呼；

（3）建立呼叫或发送短消息。

RACH 信道工作在 0 号时隙通用控制信道的上行方向，属于众多 MS 共享的资源。而 RACH 本来就是 Random Access Channel 的意思。既然是共享资源 MS 的信道请求又是随机发生的动作，网络无法实现预知。这样就会不可避免地出现多个 MS 同时要求起呼的情况。当两个 MS 在同一时隙传输时，会出现两种情况：其一是两个信号的电平相差足够大，这样网络就会处理电平较高的接入请求；其二是两个信号的电平相差不大，互相干扰，都不足以让 BTS 正确接收，这种情况麻烦就大了。GSM 的设计者从局域网的“ALOHA”协议里吸取了灵感，在 RACH 的问题上引入了重发机制。是怎样重发的呢？

当 MS 的信道请求没有被响应之前，MS 并不知道网络是否会响应它，于是在一个随机间隔的时间之后选择重发。这个时间必须是一个随机的时间而非一个固定的时间，否则开始和它发生碰撞的 MS 还会继续与之碰撞，那可大大不妙。ALOHA 协议的示意图如图 6.1 所示。

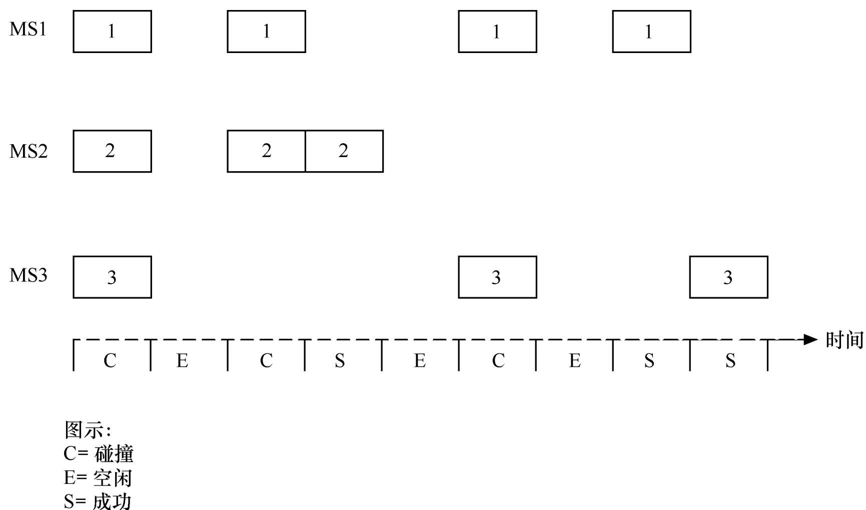


图 6.1　RACH 的碰撞与重发机制

MS1、MS2、MS3 在第 1 个 TDMA 帧的时候碰撞，只要未收到网络的确认消息，就选择随机间隔重发消息。MS2 最终在第 4 个 TDMA 帧的时候成功，MS1 最终在第 8 个 TDMA 的时候成功，MS3 最终在第 9 个 TDMA 帧的时候成功。

然而随机间隔重发并不能解决所有问题，当业务量超过一定的门限值时，重发将不

再有作用，这也是网络容量的一个重要制约因素。为了解决碰撞的问题，GSM 设计了 3 种机制。

第一种就是我们刚才所说的 ALOHA 协议的方式了，然而无限制地重发并不符合我们的预期，那只会使网络的状况更加糟糕。我们需要设置一个门限，那就是 M 参数——Maxretrans（最大重传次数，不能超过这个数目）。随机间隔时间的选取取决于“S”参数和“T”参数，连续两个 RACH 消息请求之间的时隙数是以相同的概率在{S，S+1，…，S+T−1}中选取。这两个参数的来历比较复杂，我们就不在这里展开，有兴趣的朋友可以自行查阅资料。

我们来大话一下：MS 是一个百折不挠的青年，他爱上了貌美如花的“BTS”，然后就试图向 BTS 发出约会邀请（RACH 接入）。然而 BTS 可是个大众情人，追求者是众多的。如果两个 MS 在同一时刻向她发出邀请（碰撞），要是一个比另一个优秀很多（电平值高很多），她就选择接受那个优秀的 MS 的邀请；要是两个都差不多，她就难办了，然后说：“我们下次再约吧”。两个 MS 都不笨，当然会选择一个随机的时间间隔再向 BTS 发出邀请，以避免再发生碰撞。当然即便如此，也未必就不发生碰撞，这没办法，下下次再约呗。不过人都是有尊严的，大家都有自己的心里底线，MS 的底线是“M”次一定要约到 BTS，然而第 M 次还是发生了碰撞，还是没有约成。MS 终于恼了——你就这么忙，一次机会也不给我，那好，天涯何处无芳草，我跟别人去约会好了。（超过最大重传次数 M 后，MS 判断当前小区拥塞，开始进行小区重选。）

第二种方式是当 BSC 发现没有信道分配时，就直接拒绝 RACH 上的请求消息，并在一定时间内限制被拒绝的 MS 重复接入。该 MS 的所有请求，不论是上一次的重复请求也好，用户试图发起的新的呼叫接入也罢，在一定的时间内一概通通拒绝，以减轻网络的负担。MS 收到网络的拒绝信息后，启动 T3122 计数器，并返回空闲状态，直到 T3122 逾时后才进行新的 RR 连接。

接着上面继续水煮：这回轮到 BTS 的老爸 BSC 出面了，他发现女儿实在是太火了，怕女儿挑花眼，就决定自己亲自上阵，来决定女婿的人选（接入 BSC 和 MSC）。很多 MS 是被他直接拒掉的。拒掉的理由有一大堆，比如说你年纪太大啊（TA 值超限）；老太太不同意（MSC 话务关闭）；我忙不过来，没空考察你（BSC 话务超载）；我女儿没时间（无线资源匮乏）；我女儿对你没感觉（信道激活无应答）。被拒掉的 MS 很伤心，都会去精品店买一个叫 T3122 的闹钟，这是一个倒计时闹钟。因为他们都知道 BSC 的老爸是金猪座的，一本叫《大话星座》的书说，金猪座的人记性特别不好，过了 T3122 时间，以前的事情就忘了，就可以既往不咎，所以 T3122 闹钟卖得特别火。

第三种方式是建立接入级别制，网内的用户分为 15 个级别，每个用户的级别定义在 SIM 卡和 HLR 中。正常情况下所有级别的 MS 都允许接入。当需要控制业务量时，由



BSC 决定阻塞某些接入等级，从而达到减少业务 10%、20%乃至更多的目的。处于阻塞级别的用户仍可以进行紧急呼叫。接入等级控制在 GSM 称为 AC（Access Class），这种方式的采用是极其慎重的，一般不用。GSM 的接入等级分配如下。

（1）等级 0～9：普通用户。

（2）等级 11～15：PLMN 管理、安全部门应用、公共事业部门、紧急业务、PLMN 职员。

BSC 觉得自己应付不过来这么多人，于是决定把 MS 按收入划分为 15 等级，实在忙不过来的时候干脆直接拒掉某一层级的算了，一刀切来得痛快。不过这必须很慎重的，要是传出个嫌贫爱富的名声可就不好了，呵呵！

话题到这里还不算完，这个 RACH 约会申请的理由是不尽相同的，有的只是“想和你说两句话”（发短消息），有的却是“想和你看场电影”（建立通话），对于不同的 RACH 申请，分配的时间也是不同的，对于第一种申请，给个 10 分钟就够了（分配 SDCCH 信道）；对于后一种申请，需要给两个小时（分配 TCH 信道）。问题是，MS 得先把自己的请求写清楚，BTS 美眉按照 BSC 老爹的指示精神，给了这些 MS 3 个比特用于写信道申请的理由，3 个比特可以表示 8 种信息，对于初步的判断而言，这已经够了。

然而 BTS 完全可能收到相同的申请要求，比如同时收到两张相同的小纸条，都写了“我想请你吃饭”。她得分清哪张纸条是谁写的，才好给予答复。于是那 3 个比特就不够用了，又分配了 5 个比特的随机鉴别数，用于区别不同的 MS，如图 6.2 所示。5 个比特可以区分 32 个 MS（2^5=32），应该是够用了。

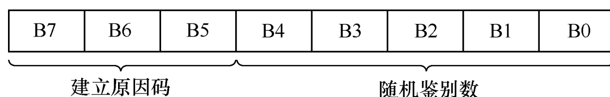


图 6.2　RACH 信道上的建立请求

BTS 收到 RACH 消息后，通过 RSM 实体的“信道请求”消息，通知 BSC，并附上 BTS 对该 MS 到 BTS 传输时延的估计，用于 BSC 初始化时间提前量（TA，Time Advance）。除此之外，消息中还可以选择增加其他信息单元，描述诸如对该 MS 的接收电平等内容。BSC 根据接入原因和当前的资源情况，选择一条合适的空闲信道，如 SDCCH 或者 TCH/F，通知 BTS 激活它。“信道激活”要求 BTS 为 MS 准备一条新的专用信道，该信道上使用的初始化时间提前量由 BSC 提供。

BTS 完成指定信道的激活后，BSC 在 AGCH 信道上发送一条立即指配消息到 MS。“立即指配消息”包含分配给该 MS 的信道描述（SDCCH 或 TCH/F 等）、初始化的时间提前量（TA 值）、初始化最大传输功率以及一个参考值。（什么是参考值呢？参考值的编排包含了 MS 在信道请求中的 8bit 以及 BTS 收到这条信息时的 TDMA 帧号。MS 拿这

8bit 和自身作一下比较，确定是不是自己发的）如果没有空闲信道可分配，BSC 就要向 MS 发送一条“立即指配拒绝”的消息，里面包含了 T3122 的值，就是我们上面说过的“T3122 闹钟”。以上内容请参见图 6.3。

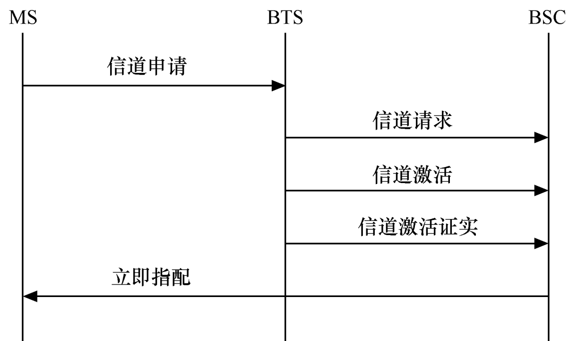


图 6.3　信道的请求与分配

当 MS 收到立即指配消息后，就把它调整到指定的信道上（SDCCH 信道或 TCH/F）信道。MS 在新的信道上做的第一件事就是发送一个 SAPI=0（GSM 空中接口数据链路层的概念，SAPI=0 对应信令）的链路层 SABM 帧（用于建立异步平衡模式），用于建立证实模式下的数据链路层连接。

这个 SABM 帧是干什么用的呢？说起来难以置信，除了说明详细的接入原因和移动台自身的状况以外，还用来确认 MS 占用该信道的正确性。因为两个 MS 发送的那 8bit 的建立原因和随机鉴别数也有可能完全相同！尽管这种概率连 1%都没有，但是我们还是要把它们区分出来。

注：根据“信道申请”原因的不同，SABM 可分为 4 种，分别是：CM 的业务请求（呼叫建立、短消息、附加业务管理）、位置更新请求（正常位置更新、周期性更新、IMSI 附着）、IMSI 分离及响应寻呼。所有这些 SABM 报文都包含了移动台的身份、接入原因、移动台的一些关键特性。我们知道，起码移动台的身份是不同的，所以 SABM 帧不会出现相同的情况。

规范采取的办法是，在 BTS 收到 SABM 帧后就会不经修改地向 MS 发送一个内容完全一样的 UA 帧，MS 通过将它本身所发送的 SABM 帧进行比对，如果一致就继续接入，否则的话就放弃该信道，重新申请信道。

BTS 在信令链路层建立之后，向 BSC 发出“建立指示”（Establish Indication）。BSC 收到建立指示后，向 MSC 申请 SCCP 连接，完整的信令流程如图 6.4 所示。

至此接入过程结束，MS 与 MSC 之间的信令链路已经建立。随着 SCCP 连接的建立，MSC 能够控制 RR 管理的传输特性，BSS 处于监控传输质量和随时准备切换的状态。



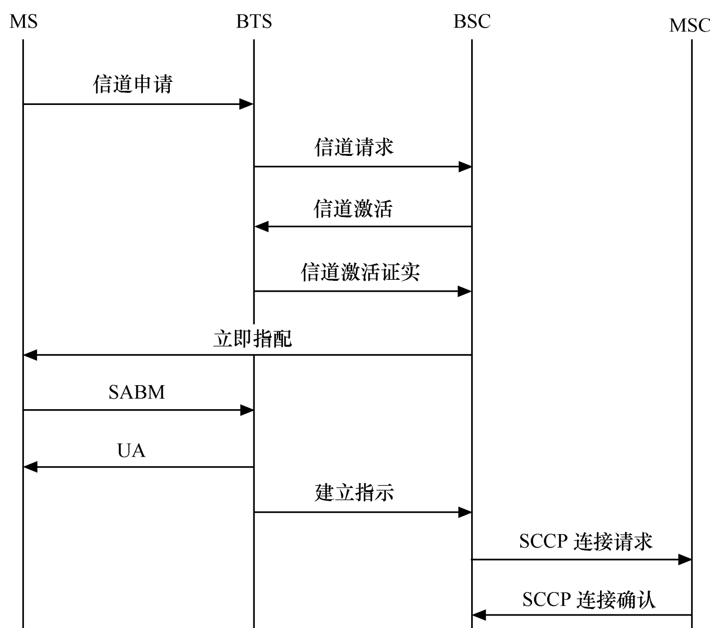


图 6.4　信道请求与分配信令流程

2. 寻呼过程的管理

寻呼我们已经在 6.2.1 节中讨论过了，这里只提一下寻呼的 3 种模式。

（1）正常寻呼模式：通常情况下都是这种寻呼方式，即由 IMSI 定义某组的寻呼消息仅在属于该寻呼组的 PCH 子信道上发送。

（2）全寻呼模式：当以这种模式下发某组寻呼时，该组寻呼消息可以在任何一个 PCH 子信道上发送。

（3）扩展寻呼模式：BSS 可以把某个分组的寻呼消息附加在另一个寻呼子信道上发送。

3. 传输模式和加密模式的管理

在 6.2.2 节中讨论过，在立即指配时，传输模式是由 BSC 选定的，RR 连接之后传输模式的选择取决于通信的需要，由 MSC 决定。MSC 可以在连接建立的任何时候要求改变传输模式，其信令流程如图 6.5 所示。

BSC 收到 MSC 的分配请求后，把 MSC 的要求和当前传输模式进行比对。如果相同，则直接向 MSC 发送“指配完成”消息；如果两者传输的信息类型不同，但信道类型一样，BSC 执行模式修改过程，然后响应 MSC 的分配请求，如图 6.5 所示；如果需要改变信道类型，BSC 就要执行一个新的分配过程，把当前连接转到要求的信道类型，然后再

应答 MSC。

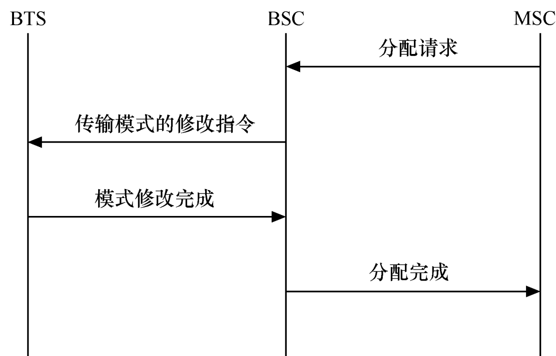


图 6.5　改变传输模式的过程

4. 呼叫重建

切换我们放到第 8 章里讨论，这里先谈谈呼叫重建，呼叫重建是切换的一种特殊情况。

与固定电话不同，手机通话过程中其信道情况，也就是无线环境是不断在变化的。在移动通话的过程中，无线传播路径中出现的高楼、隧道，可以使得接收状况骤然恶化，这被称之为大尺度衰落效应。

这种无线链路的恶化很可能造成通信中断，当采用呼叫重建机制之后，移动台便可利用本小区或者其他小区在很短的时间内恢复通话。

呼叫重建与初始接入很相似，MS 都是要重新开始申请信道，区别在于呼叫重建接入的速度必须要快。因为为了节省资源，MSC 是会把资源释放掉的，资源如果释放了，就要重新进行路由的查询和选择，MSC 和 BSC 之间的电路连接都要重建。所以只有在资源释放之前完成呼叫重建才有意义。

由于时间上的限制，规定 MS 只能选择本小区或者那些已知并且已经与 MS 建立预同步的邻小区。MS 向选择的小区发“接入请求”，原因为呼叫重建，网络识别后直接分配一条 TCH（注意，这里为了连接速度的要求，就不先分配 SDCCH 后分配 TCH 了）。

一般情况下，呼叫重建程序将持续 4～20s，多数用户在重建完成之前都已挂机，所以其实呼叫重建功能其意义是比较有限的。

5. RR 连接释放

RR 连接释放的情况有几种：第一种是正常释放，比如说位置更新结束，呼叫结束；第二种是异常释放，比如说无线链路故障等。正常的释放是由 MSC 发起的，MS 接收到 MSC 发来的信息后，释放掉占用的资源，并从专用模式转换为空闲模式。



MSC 之间的释放消息是通过 7 号信令中的 ISUP 发送的。

MSC 和 BSC 之间的链路释放是通过 MSC 向 BSC 发送“BSSMAP 清除指令”，释放掉相应的 SCCP 连接。清除之后，BSC 向 MSC 发送“SCCP 释放完成消息”。

BSC 随后通过层 3 消息通知 MS 要求其释放链路，并返回空闲模式。移动台在收到“信道释放”命令后，回送一条 LAPDm 层的 DISC（Disconnect）消息，准备断开连接。当 DISC 消息被 BTS 发出的 UA 消息证实后，MS 去活所有信道，并返回空闲模式。

BTS 发出 UA 消息证实的同时，向 BSC 发送“释放指示”。当 BSC 收到该指示后，向 BTS 发送“RF 信道释放”指令，去活（指由激活的状态变为非激活的状态，与激活对应）BTS 中相应的设备。BTS 完成后，返回一个证实消息。

上面的流程图如图 6.6 所示。

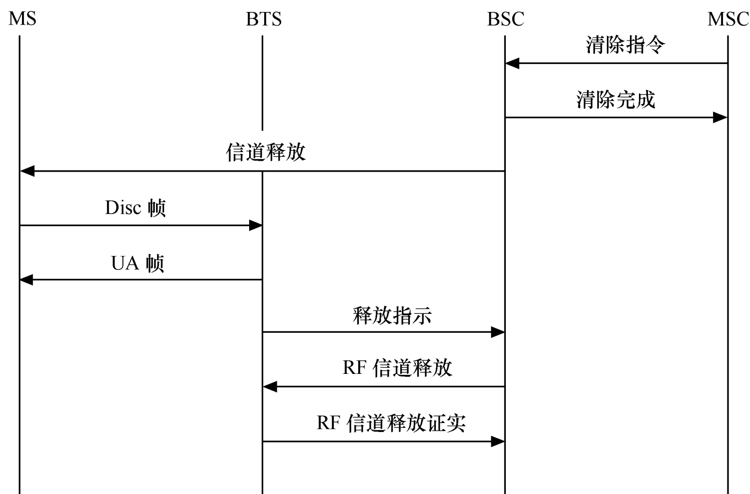


图 6.6　RR 连接的正常释放过程

6. 负载管理

MSC 和 BSC 除了负责具体的某个 RRM，对整体也要有个掌控。RRM 的一个重要内容就是 MSC 与 BSC 一起控制负载量。

BSC 需要通过 BTS 上发送和接收情况的统计，了解 RACH 和 AGCH 上的负载。BTS 通过向 BSC 发送“CCCH 负载指示”描述当前负载状态。了解了这个情况，如果出现拥塞，就便于 BSC 对 RACH 进行控制，控制的方式在本节的第 1 部分已经讨论过了。

BSC 还掌握着本小区内各类专用信道的分配情况。TCH/F 的当前使用情况可以通过“BSSMAP 资源指示”消息通知 MSC，MSC 也可以用“BSSMAP 资源请求”消息向 BSC 询问使用情况。了解这个情况的作用是用来支持小区之间由于业务过载引起的切换。

7. SACCH 过程

什么是 SACCH 呢？如果说 BCCH 是“空闲模式”下对 MS 进行信令传递和管理的一种手段，那么 SACCH 就是“专用模式”下进行 RRM 的利器！

如何才能进行 RRM，靠信令啊，SACCH 就是专用模式下传递信令用的，所以 RRM 自然与它密不可分。

在下行方向上和上行方向，SACCH 主要用来承载功率控制和时间提前量。

除此之外，SACCH 还用来传递一些无线参数，我们通常称它为系统消息（属于系统消息 5 和系统消息 6），主要包含位置区标识、小区标识、网络色码、邻近小区频点信息等内容。

发送短消息也是 SACCH 的一个功能。

8. 广播消息——系统消息

把广播消息和系统消息混在一起初看起来似乎有点不妥，因为 SACCH 消息里也含有系统消息，这个可是点对点的。可是系统消息里除了系统消息 5 和系统消息 6 是通过 SACCH 传递以外，其余都是通过 BCCH 广播的，所以在本小节中就暂时放在一起。

广播消息是发生在 RR 连接之前的，RR 连接之后都是通过 SACCH 传递消息。看起来与 RR 似乎不怎么搭界。但是广播出去的众多无线参数都对后面的 RR 连接过程产生了深远的影响，下面就来看看广播消息是如何影响 RR 连接的。

RR 在进行连接前先要选择一个小区，所以广播消息的一个重要部分是有关小区选择的处理。不仅是本小区，邻小区的这类信息也要传到 MS。本小区的频点配置是通过系统消息 1 的小区配置来描述的；邻小区的频点配置是通过系统消息 2 来下发的。

然而手机要选择一个小区并不是光知道它的频点就够了，它需要知道一系列的参数，才好决定选择哪个小区。有的在系统消息 3 下发：比如小区重选滞后（CRH，Cell Reselection Hysteresis）、控制信道最大功率电平（MS_TXPWR_MAX_CCH）、允许接入最小电平（RXLEV_ACCESS_MIN）、附加重选参数（ACS）。有的在系统消息 4 下发：小区重选参数指示（PI），小区禁止限制（CBQ，Cell Bar Qualify）、小区重选偏移（CRO，CELL_RESELECT_OFFSET）、临时偏移（TO，TEMPORARY_OFFSET）、惩罚时间（PT，PENALTY_TIME）。这些参数看得人头晕眼花，然而并不难，我们会在第 8 章中一一为大家介绍，就不在这里展开了。

上面的参数都是小区选择的内容，目的是帮助 MS 选择一个合适的小区。然而选择小区还需要知道当前小区的标识码（CGI）和位置区码（LAI），这些消息在系统消息 3 中发送给 MS。



小区选择完了，如果要进行呼叫或者位置更新，就要建立 RR 连接了，这就是 RR 管理的重要内容了。建立连接前我得知道有多少 RACH 信道，多少 AGCH 信道，还得知道有多少个寻呼子信道，好侦听属于我的寻呼信息。这些消息也在系统消息 3 中下发，包含以下几个参数：公共控制信道配置（CCCH-CONF）、接入允许保留块数（BS_AG_BLKS_RES）、寻呼信道复帧数（BS_PA_MFRAMS），这 3 个参数的内容我们在 6.3 节的第 1 部分中讲过，就不在这里重复了。

其中有一系列的参数可供选择，这就是随机接入控制参数（RACH Control Parameter），该消息在系统消息 1、2、3、4 中都下发。

随机接入控制信息主要包括以下参数。

最大重发次数（MAX retrans）：表示允许手机在收到立即指配消息前重新发送的信道请求消息的个数，即手机可以发送的信道请求个数为 M+1。它是 2 比特编码，范围 0～3 对应的最大重发次数为 1、2、4、7 次。

扩展传输时隙数目（TX_interger）：表示手机在连续发送多个信道请求消息时，每次发送之间间隔的时隙数目。

小区接入禁止（CELL_BAR_ACCESS）：指示小区是否允许手机接入，有 1 个比特编码。0 表示允许手机在本小区接入，1 表示不允许手机接入本小区；该参数不影响切换的接入。

接入等级控制（AC）：可以分为等级 0～9 和等级 11～15，一般每个 GSM 用户都有 1 个接入等级，每个等级用 1bit 来表示，该比特位 1 表示当前小区不允许具有对应等级的 MS 接入本小区，否则就允许接入。等级 11～15 比等级 0～9 的用户具有较高的接入优先级，但等级 11～15 之间或等级 0～9 之间并不表示接入优先级的高低。这个参数一般是万不得已时才采用，我们来看看阻塞 1、3、5、12 级用户应该如何设置，如图 6.7 所示。

等级	0	1	2	3	4	5	6	7	8	9	11	12	13	14	15
	0	1	0	1	0	1	0	0	0	0	0	1	0	0	0

图 6.7　AC 的接入控制

呼叫重建允许（RE）：用于指示是否允许当 MS 断话启动呼叫重建。它是 1 比特编码，为 0 表示本小区允许呼叫重建，为 1 表示本小区不允许呼叫重建。

紧急呼叫允许（EC）：指示用户在没有 SIM 卡或接入等级被当前小区关闭的情况下是否允许发起紧急呼叫。它为 1 比特编码，为 0 表示允许进行紧急呼叫，为 1 表示不允许进行紧急呼叫（但接入等级为 11～15 的用户除外）。一般而言，紧急呼叫都是允许的。

手机建立了 RR 连接以后，并不意味着 RRM 就到此为止了，我们通常还得设置

一系列参数来控制它的传输行为。这些参数也在系统消息 3 中发送，主要有以下几个参数。

非连续发送（DTX）：指 示 MS 是否可以使用 DTX 功能，在系统消息 3 中为 2bit 编码，在系统选项 6 中为 3bit 编码。

无线链路超时（Radio_Link_Timeout）：用来判断 RR 连接是不是断了，是一个 4bit 编码，范围 0～15 对应数值 4～64。当 MS 每收到一个正确的 SACCH 信息时，该值加 2；当 MS 在应收到 SACCH 消息的时刻无法解码出一个正确的 SACCH 消息时，该值减 1；当该值为 0 时，MS 向基站上报无线链路故障。

无线链路故障的图示如图 6.8 所示。

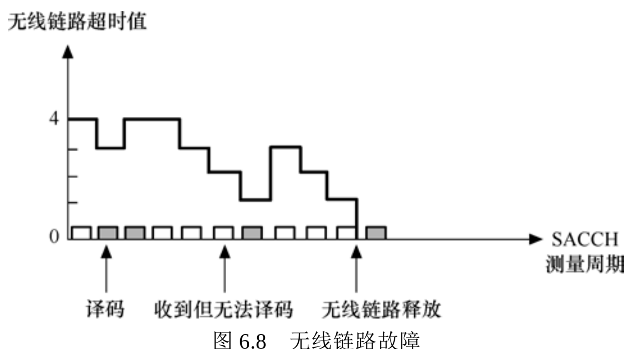


图 6.8　无线链路故障

请注意，我们刚刚对系统消息的描述是按手机的行为进行排序的，首先是从系统消息 1 和系统消息 2 中得知当前小区和邻小区所使用的频率。然后通过系统消息 3 和系统消息 4 下发的一系列参数来进行小区重选。对于呼叫建立和响应寻呼而言，位置区识别码 LAI 和小区识别号 CGI 显然是很重要的，这个是通过系统消息 3 下发。对这些因素都清楚了之后，MS 开始考虑进行 RR 连接，RR 连接之前的必修课是搞清楚所在小区到底有多少 RACH 信道可以接入，当然，要当被叫的话，知道有多少寻呼子信道显然也很重要，否则怎么知道去哪个信道监听寻呼呢？这都需要系统消息 3 告诉它。搞清楚配置之后，剩下的工作就是接入了，对于接入而言，一个重要的 RRM 工作是进行拥塞控制，我们在本节第 1 部分讲过拥塞控制的方法，又在上面列举了所需的参数。另外，建立连接后，我们还需判断是否进行非连续发射（DTX）以及链路是否已中断（Radio_Link_Timeout）。

下面我们从另一个角度来描述系统消息，那就是按系统消息本身的排列方式来进行描述，从系统消息 1 描述到系统消息 8。刚才的叙述方式是把系统消息打散了进行阐述的，现在我们把它合起来，做一个概括和总结，以便读者有个整体的概念。

在 GSM 移动通信系统中，系统消息的发送方式有两种：一种是广播消息 BCCH，



另一种是随路消息 SACCH。系统消息包含了空中接口上的主要无线网络参数，具体包括了网络识别参数（识别运营商）、小区选择参数（选择一个合适的小区）、系统控制参数（描述通用控制信道以及随机接入信息）和网络功能参数（对功率进行控制，对链路情况进行判断）。

广播消息和随路消息是紧密相连的，两者的信息有很大一部分是重叠的，不过一个用于空闲模式，一个用于专用模式而已。

网络不断通过 BTS 给所有的 MS 发送一些消息，这些被称为系统消息。在 GSM 网络中，根据消息内容的不同和传送信道的不同，而把系统消息分为以下几种类型。

（1）系统消息 1：主要描述了小区频点分配（CA）表和随机接入信道（RACH）信息。

（2）系统消息 2：主要描述了邻小区频点分配（BA）表、随机接入信道（RACH）信息和网络色码允许（NCC Permitted）。

（3）系统消息 3：主要描述了位置区标识（LAI）、小区标识（CGI）、随机接入信道（RACH）信息以及和小区选择有关的参数、小区功能描述（DTX、无线链路超时）。

（4）系统消息 4：位置区标识（LAI）、CBCH 信道描述、随机接入信道（RACH）信息以及和小区选择有关的参数。

（5）系统消息 5：这些消息通过 SACCH 信道下发，主要描述了邻小区频点分配表（BA 表）。系统消息 5 与系统消息 3 的主要区别就是没有了随机接入信道（RACH）信息以及和小区选择有关的参数，因为此时已经建立了 RR 连接，所以以上两项内容就不再需要了。

（6）系统消息 6：主要描述了位置区标识（LAI）、小区标识（CGI）、网络色码允许（NCC Permitted）以及一些描述小区功能的参数。系统消息 6 与系统消息 4 的主要区别也是没有了随机接入信道（RACH）信息以及和小区选择有关的参数。

（7）系统消息 7：我们在上面没有提过该消息，这个消息在 BCCH 上发送，包含用于该小区重选的信息。

（8）系统消息 8：这个消息在 BCCH 上发送，包含用于该小区重选的信息。

6.3 移动性与安全性的博弈——移动性管理（MM）

不能说固定电话就有多么安全，固定电话在线路上是明码传输的。另外，交接箱也是一个薄弱环节，即使到了现在也是如此，我们经常可以看到这样的新闻："某某警方破获某地盗打固定电话系列案"。这类案子一般有两大特点，一大特点就是通过固定电话给

某些网络增值业务进行充值，因为现在电话费便宜了，谁都不差打电话的那几个小钱，盗打电话的目的都是用来给点卡充值好去淘宝上卖钱。另一大特点就是被攻破的环节往往是交接箱。

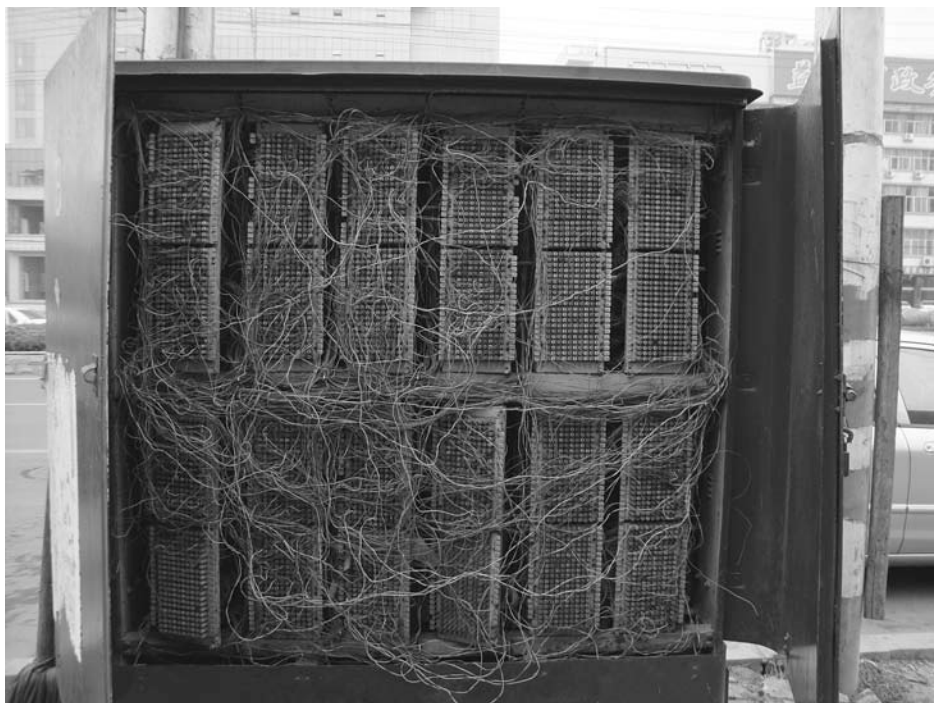


图 6.9　电话交接箱

虽然如此，固定电话相对第一代模拟通信而言，还是要安全得多的，要动交接箱不难，就在图 6.9 所示箱子的那些口子上插根线就可以打电话。难的是交接箱都竖在路边上或小区里，众目睽睽之下犯罪风险还是蛮大的。所以说固定电话相对而言还是比较安全。

到了移动通信时代（特指 1G 模拟通信时代）情况就大不一样了，电磁波就在空中四散传播，架根天线谁都能收到，这可不像固定电话信号只在电话线里传输。要命的是移动台的鉴权方式又简单，只有一个移动识别号（MIN，Mobile Identification Number）和一个电子序列号（ESN，Electronic Serial Number），所以电话被人破解盗打的案例可不少。再者是模拟信号根本就不加密，嗨嗨，人家用天线接收后那可听得是一清二楚啊，就像当年的小霸王学习机一样，你邻居在家里打游戏，你打开电视那画面可是看得清清楚楚，这就是模拟信号用于通信的最大弊端。电视用模拟信号无所谓，毕竟是公共的，电话可是私密行为啊。



我们刚刚所说的是从用户的角度来理解安全性，那么从运营商的角度而言，安全性也是极为重要的。运营商是从以下几个角度来理解安全问题的：一是对用户身份的确认，这对移动运营商的商业模式而言非常重要，如果按照固定电话的方式，仅仅以用户号码来确认身份，而不考虑别的因素，那就会出大问题。这个问题为什么这么讲呢，因为固定电话采用那样的身份识别模式和计费模式，是有其隐含条件的，这个隐含条件就是号码与别人家里墙上的电话接口是一一对应的，我知道你是谁，我能收到你的费，你跑得了和尚还能跑得了庙？并且，这个号码是没办法伪造的，要伪造的话你得先去打开交接箱自己插根线上去，当然这属于比较极端的情况，不在考虑之列。而对移动通信而言，这样简单的鉴别方式就完全不奏效了。首先，如果只简单地照搬固定电话用号码对用户进行鉴别的话，那么这个系统也太脆弱了。因为固定通信的信号都是在电话线里传递的，要和网络进行联系你得先进交接箱的，交接箱的钥匙你是没有的，运营商不让你进你就没辙。移动通信就不一样了，信息是通过电磁波传递的，电磁波显然谁都可以发送，移动通信也没有什么交接箱，只有一个 BTS 负责接收信号，BTS 就只有一根傻傻的天线，它可是谁的信号都照收不误。如果只用电话号码来鉴别身份，这个号码与人家家里的接口又没有一一对应关系，那通信运营商就等着被盗打电话的黑个天昏地暗吧。这个可不用冒险去交接箱里接线，只要在家里发射电磁波就行了。

我们上面已经论证了固网的那一套鉴权方式对移动通信而言是行不通的，关于移动通信的鉴权方式，会在本节后面的内容加以讨论。

至于固网的加密方式，也同样有点防君子不防小人的意味。固网的信号在线路上都是明码传输的，只要你能打开交接箱，那剩下的工作和盗打电话一样简单。不过固网也有一个好处，就是它的信号只是在电话线或者同轴电缆上传输，不像移动通信一样电磁信号是四散传播的。电磁波的这种传播特性要了移动通信的命，如果不进行加密，真的是别人竖一根天线加一部接收机就可以完成窃听。与固定电话不同的是你还根本不知道人家在哪里窃听你，都没法去抓，这个费用成本和违法成本也太低廉了！模拟通信无法很好地加密或许是它被数字通信迅速取代的原因。作为服务行业的企业，用户的需要就应当是运营商的工作，用户既然对模拟通信时代被窃听电话的经历深恶痛绝，那么有效地对用户信息和通话进行加密也就是一个成熟的商业无线通信系统所必备的功能。

我们看到，无论是鉴权还是加密，固网的那套方式对于移动通信而言都已经彻底破产了。移动通信相对固网由于可以“移动”而产生了本质的不同，所以说安全管理方式的变化其实是源于移动性。这也许就是我们把鉴权和加密纳入移动性管理（MM）的理由吧。

除了安全性的管理，MM 的重要任务还有对 MS 所在区域的管理。这项工作显然很重要，因为如果不对区域进行很好的划分和管理，系统就不知道你在哪里，不知道你在哪里就没法对你呼叫，网络没法对你进行呼叫你就没法当被叫，大家都当不了被叫，主叫又有什么意义呢，难道自己和自己通话吗？

下面就对 MM 的两个方面——位置区域的管理和安全性的管理进行讨论。

6.3.1　位置区域的管理

对位置区域的管理比较宏观的考虑因素就是 GSM 网络与网络之间的互通。这是一个相当重要的工作，因为 GSM 网络是一个全球网络，一个国家的网络与另一个国家的网络之间是必须要能够互通和漫游的。如果说 CGI 和 LAI 的管理是位置区域的微观层面的管理的话，那么互通和漫游就是位置区域宏观层面的管理了。

由于 GSM 规范源于欧洲，所以在系统管理方面也深深地印有欧洲电信系统的影子。欧洲的 GSM 系统分为若干个独立的运营网，称为 PLMN。通常一个 PLMN 只覆盖一个国家，那么要对得起 GSM（Global System for Mobile communications，全球移动通信系统）这个称号自然要实现不同 PLMN 的漫游。PLMN 之间要实现互通有几个条件：首先，PLMN 之间要能通信，要有一个标准的通信协议才能互连；其次，就是 SIM 卡要能在不同的 PLMN 网中实现注册。GSM 每个用户都在一个 PLMN 网建立注册关系，称这个 PLMN 为用户的归属 PLMN 网。用户的注册信息除了个人信息之外，还包括所选的业务类型，以及指定的可以使用的范围（本地、全国漫游、国际漫游）。

我们上面讨论了宏观层面的 PLMN，下面讨论一下微观层面的位置区域内容。

VLR：通常 VLR 和 MSC 结合在一起，控制 MSC 下所有小区的临时用户的注册，这些小区覆盖的区域称为 VLR。

LA：LA 是位置区的意思，LAI 是位置区标识，后者是前者的标识号。MS 的位置更新是在 LA 之间进行的。一个 MSC 下面通常有若干个 BSC，通常把某个 BSC 下控制的所有小区分为一个 LA。LA 之间的分界通常建议选择业务量不是很大的区域，如果业务量很大的话，那么位置更新必然也很多，会给网络带来很大的信令负荷的压力。

小区：一个 BSC 下通常有若干个 BTS，一个 BTS 通常有 3 个小区。

以上区域的划分详见图 6.10。

LA 区的划分在一个 MSC 里是可大可小的，但这个工作并不好做。划大了可以减少位置更新的信令负荷，同时也会增加寻呼的信令负荷，寻呼和位置更新在这个层面而言是一对矛盾，我们需要在两者之间寻找一个平衡点，但其根本目的却是一致的，就是希望减少总体的信令负荷和资源浪费。

MS 必须通过 SIM 卡注册当前的 VLR，VLR 从 HLR 里调取用户的相关数据，才能



够获得服务。注册的过程先是要选择 PLMN（选择运营商），然后进行小区选择（选择一个与之通信的小区），小区选择的规则主要来自无线传播条件，打电话的时候我们肯定希望选择无线环境最好的小区。小区选择的具体过程我们会在第 8 章里进行详细介绍，就不在这里展开了。

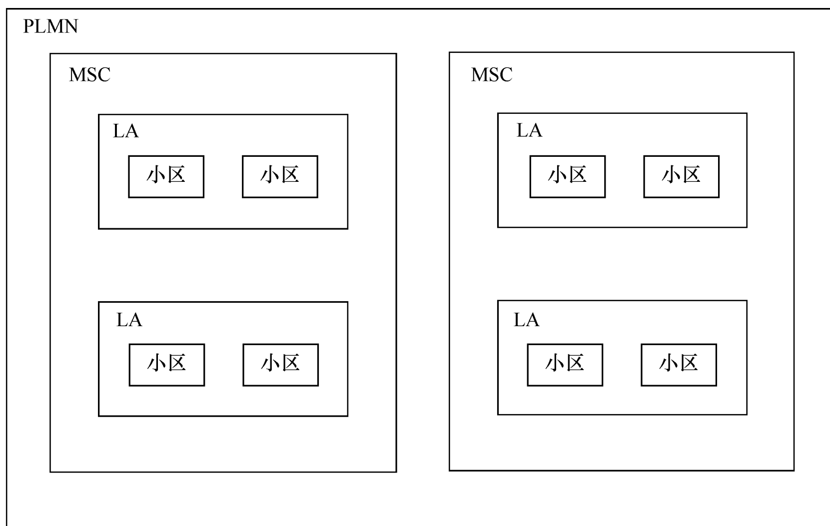


图 6.10　GSM 中业务区域的划分

1. 位置区的划分

选择 PLMN 和小区只是移动性管理的一部分，而其最终目的是与移动的用户建立呼叫连接。网络必须记录每个 MS 的资料（SIM 卡）和所在的位置区，只有知道这些信息，MSC 才能建立起有效的连接，在相应的位置区内进行寻呼。至于寻呼后该怎么做，那是 RR 层面需要考虑的问题，我们在上一节中已经讲过了。

对于位置区的管理基本设想是要建立一个数据库，其中存有每个用户的标识以及是否注册、如何找到等信息。GSM 和其他通信系统一样，都需要一个基本的用户数据库，记录诸如用户权限、附加业务选择、计费等信息。在固定通信中，墙上的接口把用户连到交接箱，交接箱将该线路连入一个本地交换局，不论呼入还是呼出，这个局地址是不变的，因此很自然就把用户资料存入这个本地局，这是固定通信的做法。

我们知道，GSM 作为一个无线通信系统，在很多方面的思路其实还是沿用固网的。GSM 对用户信息的储存也采用了类似的方法，它把用户的资料以及当前所在的 MSC/VLR 信息存储于 MSC，前者是静态的信息，而后者是动态的信息。位置区信息往往只用于建立移动被叫，而用户信息在整个呼叫过程中都需要。

然而用户的资料信息是相当多的，什么 MSISDN、IMSI、Ki、接入的优先等级、补充业务，那是啰啰嗦嗦一大串。而这些资料又只有 MS 当前所在区域的 MSC 需要，如果每次呼叫，MSC 都要去 HLR 把这一堆数据搞回来，那么信令负荷可不是一般的大。这就跟 DNS 一样，如果各个 ISP，比如中国电信、中国联通、长城宽带以及广电宽带，它们要是没有本地 DNS 缓存信息，每次上个网还真得从根 DNS 一级级查数据，一准得把根 DNS 累瘫。鉴于此，MSC 下面建立了一个称为拜访位置寄存器（VLR）的数据库，管理那些处于当前 MSC 管辖下全部 LA 内的当前用户资料。这个临时数据库，存储了精确的用户位置（LAI）以及从 HLR 下载的用户的相关资料，可以把这个 VLR 理解为 HLR 的本地缓存好了。每当 MS 由一个 MSC/VLR 进入另一个 MSC/VLR 时，它又从 HLR 里把数据下载到新的 VLR 里面，然后要求原来的 VLR 把相关的信息删掉。MS 都不在你那里了，你还存着别人的东西，多占地方啊。

2. 位置更新

位置更新的主要目的就是为了做被叫，网络是没有雷达的，它并不能看到某个 MS 现在处在哪个位置。MS 到了新的位置区如果不主动把相应的位置信息告诉网络，那么网络就无法对它进行寻呼从而找到它。

上面所说的是位置更新必须由 MS 触发，就像当年没有手机的时代你出去玩一样，你必须提前主动向你老妈汇报你的位置，要不然你老妈不知道你去了哪里了，现在又在何方，相关内容可以参见第 1 章。

在 GSM 系统中，有 3 个地方需要知道信息位置，即 HLR、VLR 和 MS，HLR 是不需要知道 MS 具体所在的位置区的，HLR 就是一建立 NSS 侧路由的功能，BSS 侧的路径是不需要 HLR 操心的。

位置更新的目的是为了能够知道手机目前所在区域，从而能够对它寻呼。那么我们就会发现，光靠改变了位置区就上报新的位置信息这一点是达不到这样的要求的。比如说手机进入了盲区，信号都没有，当然不会有位置更新，这时候你还对它做寻呼当然是浪费系统的资源。对这个问题我们怎么解决呢？GSM 设置了一个叫做 T3212 的小区参数，要求 MS 定时上报自己的位置信息，这个称之为“周期性更新”，假如把 T3212 设置成 30 分钟，过了 30 分钟你还没向我上报位置信息，我管你是手机电板被拔了还是进入了网络盲区，我就默认你已经“无网络”了，然后在 MSC/VLR 上做个标记，再有呼叫过来，我就不对你进行寻呼了，要建设节约型社会嘛，资源是不能随便浪费的。正常的位置更新和周期性位置更新加在一起，基本就解决了做被叫的大部分问题。但还是有个问题令我们不能容忍，进入网络盲区和手机电板被拔出来的情况毕竟还是很少的，但是大家的手机基本每天都会要关一次机，我关机后按周期性更新来说要 30 分钟之后网络



才知道我的手机关机了，全国这么多手机，得造成多大的浪费？不行，我们得想个办法，GSM 的设计者想到的就是开关机的时候都通知网络一声，这称为“IMSI Attach/Detach”，当 MS 切断电源关机的时候，MS 向网络发送最后一条信息，即分离处理请求（IMSI Detach），MSC 接收到后，即通知 VLR 对该 MS 对应的 IMSI 上作“分离”标记。该用户脱离网络的消息并不发给 HLR，如果该客户被其他用户呼叫时，HLR 会向该用户当前所在的 MSC/VLR 要漫游号码 MSRN 用于建立连接，MSC/VLR 此时会通知 HLR 该用户已脱离网络，不需要进行寻呼。当 MS 又重新开机时，如果通过接收系统消息发现开机时的位置区标识（LAI）已经发生了改变，那么就执行正常的位置更新，如果位置区没有发现改变，那么就只向网络发送一个“附着”信息，告诉网络我又回来了，可以对我进行寻呼了。

我们在上面简单地讲了位置更新的 3 种方式：正常位置更新、IMSI Attach/Detach 以及周期性位置更新。3 种位置更新其根本目的都是为了更好地完成被叫工作，我们还会在第 8 章详细讲解这 3 种方式的信令流程。

6.3.2　也谈 SIM 卡的破解——安全性管理

如果手机也像固定电话一样牵着一根电话线，而不是用电磁波四散发射的话，或许就不会有这么多麻烦。既然我们需要用电磁波来承载信号，既然用户的身份无法再用电话号码以及墙上的接口来一一对应，我们就需要重新审视我们的系统构架，并解决这些潜在的安全问题。

前面说过 MSISDN 就像姓名，我们平时用姓名互相称呼彼此，用电话号码来联系这部手机或者那部手机。但真正在 GSM 网络里通用的用户识别号却不是这个，是 IMSI，用户身份的鉴权也好，路由的寻址也罢，都是用的 IMSI。MSISDN 仅仅用于用户之间的识别，到了网络侧，MSC 会把它翻译成 IMSI 再用。如 4.8 节所述，这有点类似身份证上的姓名和身份证号，朋友和朋友之间互相称姓名，但是公安机关或者民政局就要看你的身份证号了，他们那个体系是用身份证号来唯一识别和管理公民的。

身份证是一定要鉴权机制的，否则你自己伪造一张身份证然后填个身份证号就可以在社会上招摇撞骗了。身份证的鉴别方式有很多种，比如说“真身份证正面‘性别’字样下的国界线有 3 处未连接的缺口；假身份证此处无缺口”、“真身份证反面国徽天安门下方的齿轮中心为圈状。若齿轮中心圈中为‘1’形状，一定是假身份证。”种种方式不一而足，这些信息公安机关都是公开告诉大众的，然而公安机关却绝不会告诉你这些细节在技术上是怎么实现的。与此类似，GSM 鉴权的实现机理 GSM 组织也是公开的，我们都知道 GSM 的密匙叫做 Ki，鉴权算法叫做 A3，然而 GSM 组织是决计不肯告诉你 Ki 是怎么得来的，A3 算法的细节是怎样的。道理很简单，谁告诉你谁傻瓜，等着你学会算

法然后去破解网络啊？

所以作为初学者的我们，是不必去搞清楚 Ki 和 A3 的细节的，人家也不会让你搞清楚。但是我们必须知道鉴权的机理，这是 GSM 网络的重要构成环节，要是鉴权都没有了，那么运营商都找谁去收费。

在 4.7.4 节中已经讨论过 GSM 的鉴权机制，所以在下面我们只打算把鉴权的图列出来，一些具体的内容就不再进行重复。在本节中，我们感兴趣的是，这个鉴权机制究竟有没有用？为什么有用，可不可以破解？该如何破解？

SIM 卡里有 3 组数据是很关键的，IMSI 号、ICCID 号和 Ki 号，有这 3 组数据，就可以复制一张 SIM 卡。ICCID 号就是 SIM 卡号，这个序列号就印在卡的背面，IMSI 号也是可以通过 SIM 卡接口读出来的，只有 Ki 号是加密的，无法通过 SIM 卡接口读出来，在这个呼叫的过程中，Ki 号也不在网络的任何一个环节（无论是空中接口还是有线链路上）进行传递。因此在整个鉴权的环节，最关键最核心的一环就是密匙 Ki 号了，Ki 号是一个 16 个字节的加密数据，16 字节就是 128bit 了，在网络侧的 AUC 里，也有一份这样的数据。

GSM 的加密系统里面大致涉及 3 种算法，即 A3、A5、A8，这些并不特定指代什么算法，只是给出算法的输入和输出规范，以及对算法的要求，GSM 对于每种算法各有一个范例实现，理论上并没有限制大家使用哪种算法。但是运营商之间是需要漫游的，一个运营商搞一种算法显然不太合适，所以大家就偷懒采用了相同的算法，于是全世界的 SIM 卡的破解方法都一样了。

在手机登录移动网络的时候，移动网络会产生一个 128bit 的随机数据（通常称为 RAND）发给手机，手机将这个数据发给 SIM 卡，SIM 卡用自己的密钥 Ki 和 RAND 做运算以后，生成一个 32bit 的应答（SRES）发回给手机，并转发给移动网络，与此同时，移动网络也进行了相同算法的运算，移动网络会比较一下这两个结果是否相同，相同就表明这个卡是我发出来的，允许其登录。这个验证算法在 GSM 规范里面叫做 A3，m=128 bit，k=128 bit，c=32 bit，这个算法要求已知 m 和 k 可以很简单地算出 c，但是已知 m 和 c 却很难算出 Ki。（该结论源自本书参考文献 3 中对 Diffie-Hellman 密钥交换算法的论述。）A3 算法是做在 SIM 卡里面的，因此如果运营商想更换加密算法，只要发行自己的 SIM 卡，让自己的基站和 SIM 卡都使用相同的算法就可以了，手机完全不用换。

从图 6.11 所示的鉴权流程图里我们可以清楚地看到 A3 算法和 Ki 是破解 SIM 的关键。问题是 A3 算法是保密的，Ki 大家也是不知道的，那些玩一卡多号的人是如何做到复制 SIM 卡的呢？



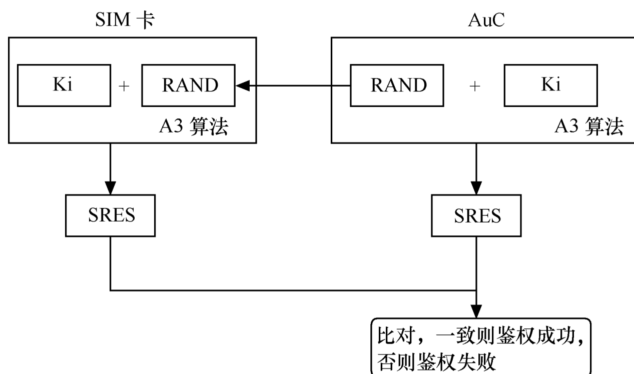


图 6.11　鉴权流程图

A3 算法一直是作为高级商业机密被保存起来了，有几页文档被偷了出来并被输入了电脑，这些资料后来落到了加州伯克利大学几个教授手里。加州伯克利大学是啥地方啊，学计算机的都知道那是一所超级牛校，诺贝尔奖得主都是一堆，可不是吃素的。这些教授拿了这些资料与 SIM 卡比对计算，硬生生把这个算法的本来面目还原了。于是这个算法就被流传了出去，称之为 Comp128 算法。

A3 算法被破解了，剩下的事情就是对付 Ki 了。说到破解某个密匙，大家一般最先想到的就是暴力破解——穷举法。GSM 的设计者也不是傻子，早就知道会有这么一天，于是在 SIM 里设计了一个逻辑电路，电路的核心内容就是 SIM 卡只能被查询 2 的 16 次方，超过这个次数 SIM 卡就会自杀，让暴力破解者啥都得不到。（当然，次数太低了也不行，每次呼叫、位置更新乃至更新卡上的电话簿都需要读取 SIM 卡）我的 Ki 号可是有 128 位哦，想穷举我就请运行 2 的 128 次方，哼哼！啥，你打算 2 的 16 次方就想破解俺，那就得看你有多大本事了。

这么一个招数让这群黑客很郁闷，他们因此不得不试图在可以接受的次数之内通过构造特定明文和分析输出密文来分析出 Ki 的值，结果还真被大家发现出来了一些，IBM 的一个小组甚至用 6 次查询就可以彻底解出 Ki。

随着时间的推移，针对 Comp128 的破解算法越来越成熟，SIM 复制设备也越来越多，运营商终于坐不住了。很多运营商都开始发行 Comp128 v2 加密算法的卡了。Comp128 v2 算法是 GSM 协会在 v1 被攻破以后，迅速在 v1 上面修改得来的结果，据说比较好地解决了 v1 算法中的弱点，当然，这个算法像 v1 一样，还是不公布于众的，而且到现在也没有人公布出来。这样一来，目前来看 SIM 卡的安全是得到了保障了。

至于加密用的 A8 算法，真的没有什么太多好说的，大家先看看 A8 算法的图，如图 6.12 所示。

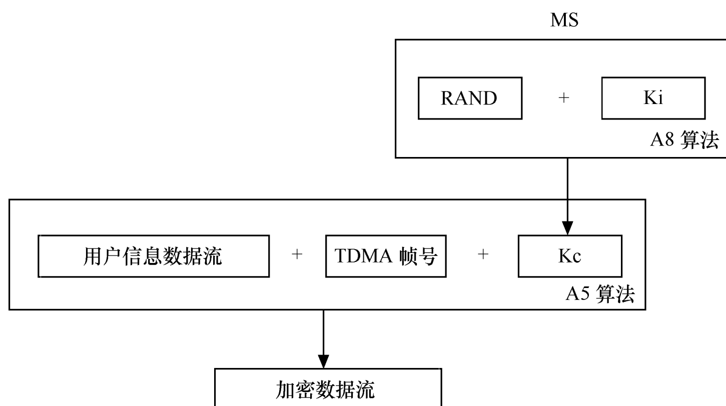


图 6.12　A8 算法

不知道大家看这张图发现诀窍没有，A3 算法和 A8 算法的输入完全一样，都是 RAND 和 Ki 号。这个世界懒人是如此之多，GSM 的设计者就在这个上面偷了个懒，他们用一个算法生成了 SRES 和 Kc，这个算法就是我们刚刚所说的 Comp128 算法。

随着 v2 版本的推出和对 v1 的逐渐替代，一卡多号，复制 SIM 卡的在逐渐减少，但谁知道 v2 是不是也有一天会被人破解呢，拭目以待吧！

6.4 从路由到计费——接续管理（CM）

我们在本章开篇的时候就说过，接续管理（CM）是基于 RRM 子层和 MM 子层之上的，要做好物流工作，首先得修好高速公路并维护好这条道路（RRM），RRM 很大一部分作用是弥补无线通信相对有线通信的一大缺点：没有一条已经建立好的稳定的链路，从 RACH 连接到功率控制到无线链路故障判别，为了解决这个问题，不但要有一条链路，而且要稳定，要能判断是否出了问题；路修好之后自然要建立收费站用来做好进出车辆的鉴别和收费工作（MM，只有买票的合法用户才能上高速），至于在此之上如何高效地完成点对点的物流运送工作，那就是 CM 的事情了。

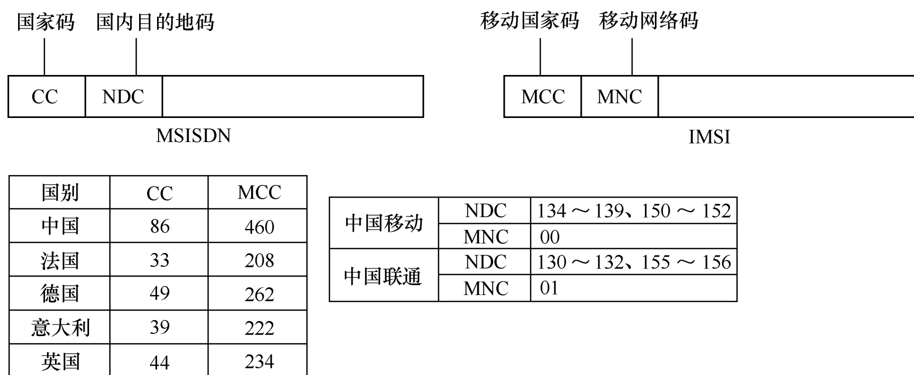
CM 的主要工作是建立主叫和被叫点对点的通信链路以及呼叫完成后对这条链路进行拆除。由于主叫和被叫的信令流程我们会在第 8 章里提到，因此在这里我们把关注的焦点放到两个方面：其一，通信运营商要活下去，必定要计费，那么长途、国内漫游、国际漫游的收费原则都是怎样的；其二，CM 实施的基础是要找到点对点通信的路由，那么如何查询到正确的路由自然相当重要。



6.4.1　也谈路由的查询——MSISDN 与 MSRN 的索引功能

GSM 系统中移动用户使用的电话号码称为 MSISDN 号，是按 CCITT 的建议书 E.164 提出的方法进行编号的。与此相同的还有移动用户漫游号 MSRN，这个号码无论是主叫还是被叫都是看不到的，它的作用仅仅是指出被叫用户所在 MSC/VLR 的路由，并且是每次呼叫时由系统临时分配的。

GSM 系统中使用的另一种号码是国际移动用户识别号 IMSI，它是 GSM 系统数据库中用以识别每个用户的号码，就是我们之前一再说过的“身份证号”。无论是 MSISDN 号还是 IMSI 号都包含了对国家以及国家内移动通信网的识别号，也就是说，你可以根据这个号码判断它是哪个国家哪个运营商的。MSISDN 用于判断国家的是 CC（Country Code，国家码），用于判断运营商的是 NDC（National Destionation Code，国内目的地码）；IMSI 用于判断国家的是 MCC（Mobile Country Code，移动国家码），用于判断运营商的是 MNC（Mobile Network Code，移动网络码）。我们下面就来看看具体是怎么判断的，如图 6.13 所示。



国别	CC	MCC
中国	86	460
法国	33	208
德国	49	262
意大利	39	222
英国	44	234

中国移动	NDC	134～139、150～152
	MNC	00
中国联通	NDC	130～132、155～156
	MNC	01

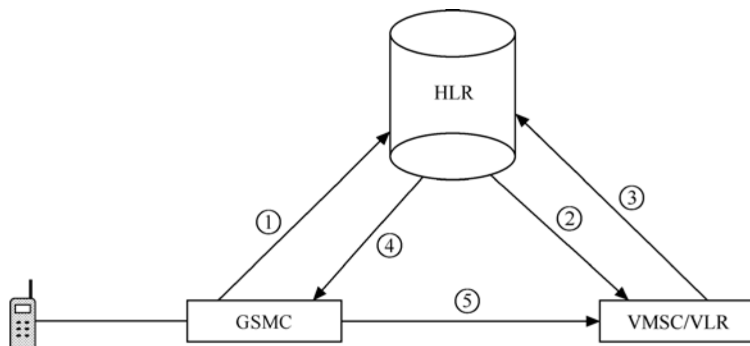
MSISDN 的 CC 码按照 CCITT E.164 建议书
IMSI 的 MCC 码按照 CCITT E.212 建议书

图 6.13　IMSI 号与 MSISDN 号国家码与网络接入码的不同

上面提到的 CC/MCC、NDC/MNC 其作用在于识别所属国家与运营商，对于具体的路由而言，这还是很空泛的概念，对于网络侧 NSS 而言，我们的寻址是要做到找到终端局 MSC/VLR。上面已经说了，被叫用户当前所在的终端局 MSC/VLR 的寻址地址是通过 MSRN 漫游号来识别的，那么主叫方是怎么知道被叫用户的这个漫游号的呢？这还得从号码分析开始。

国内的移动号码通常是 13×H0H1H2H3ABCD 的格局，大家可以发现，中间 4 位数 H0H1H2H3 相同的必定是同一个城市的，这也是所谓的号码归属地分析软件的工作机理。这个 H0H1H2H3 做什么用呢？用于识别用户归属的 HLR，然后通过查询 HLR 就可以确定到达该移动用户的路由，找到路由后就可以建立起呼叫连接。由此可见，整个呼叫建立也

可以分为两部分：查询路由与建立连接。查询的路由也分为两段：从 GMSC 到 HLR 是第一段路由，从 HLR 到 VMSC 是第二段路由。整个呼叫建立工作的示意图如图 6.14 所示。



其中步骤①②③④都是用于查询路由的，步骤⑤是用来连接 GSMC
和终端局 VMSC（Visited MSC，被访问的 MSC）的。

图 6.14　路由查询过程

在这里，我们需要解释一下什么是 GMSC，说起 GSMC，其实与 MSC 没有什么关系，它是网关移动交换中心（Gateway Mobile Switching Center）的意思，其作用就是路由的转接，并不涉及移动交换功能。但是现在网络的现状，通常是这个 GMSC 与 MSC 合并在一起了。下面我们讲讲具体的 5 个步骤。

GMSC 经过对被叫号码里的 H0H1H2H3 进行分析，可以得知该号码的归属位置寄存器 HLR，然后就要向 HLR 发送信息。

步骤①：GMSC 向 HLR 发送被叫到 MSISDN。

步骤②：HLR 分析 MSISDN，找到对应的 IMSI 号和所在的 MSC 地址，并向该终端 MSC 发送被叫的 IMSI 号，要求 VMSC 提供一个 MSRN 号以供建立呼叫。

步骤③：VMSC 找到一个空闲的 MSRN，配给该 IMSI 用户，并向 HLR 提供该 MSRN 号。

步骤④：HLR 向 GMSC 返回该 MSRN 号。

步骤⑤：GSMC 根据 MSRN 号判断出 VMSC 的地址，然后建立连接。

在 4.8 节中，我们有对上述过程的图例，大家可以看看。

6.4.2　漫游费的由来

漫游费引发的争论在这些年就从没消停过，本小节并不打算参与其中的口水战。作为一个移动通信的从业人员或者即将从业的人员，了解移动通信计费和漫游计费的机理才是正经要做的事。

谈到计费原则，我们又不得不提到固网，这并没有什么好奇怪的，因为固网本来就是现代通信网的鼻祖，移动通信的很多理念，尤其是网络侧 NSS 的理念乃至协议都来自固网。



众所周知，固网的被叫是不收费的，而移动通信的被叫一直是收费的，为此不知道有过多少争论，直到最近一两年手机才逐渐实行单向收费，这是一次“消费者—国资委—运营商”三方博弈均衡的结果。而我们想问的是：“移动通信的被叫到底比固定电话的被叫多了哪些成本，从而导致这么多年来运营商一直是向被叫收取费用的”？其实移动台作为被叫和固定电话作为被叫最大的区别就是—固定电话所在的位置和路由是已知的，而手机所在的位置和路由是未知的，需要进行查询。我们下面来看看手机和固话作为被叫进行寻址的对比图（见图 6.15 和图 6.16），看看区别在哪里。

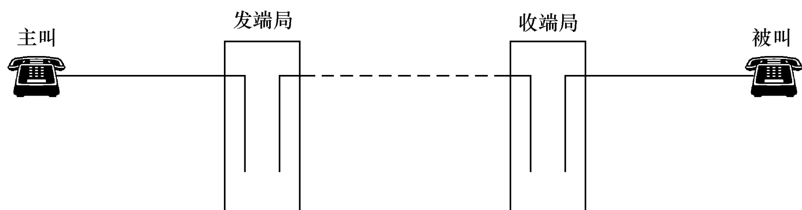


图 6.15　固话的寻址

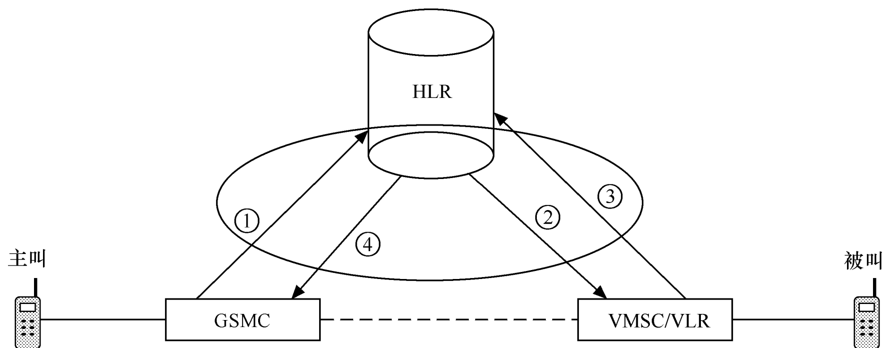


图 6.16　移动网的寻址

从图 6.16 我们可以看出，圆圈所示部分就是移动网与固定通信网的最大区别，移动通信由于不知道被叫所在的位置，需要去 HLR 查询，需要 VMSC 向 HLR 回馈 MSRN 号，也就是我们之前所说的步骤①②③④，这就是当年运营商对被叫收取费用的逻辑。有人或许要问，为什么这段费用不向主叫收取呢？之所以要进行路由查询，是因为被叫位置的不确定性，不是因为主叫位置的不确定性，您要漫游到马尔代夫别人要找您的话那铁定要去查询马尔代夫的 VMSC 了，人家主叫也不是您肚子里的蛔虫，人家也不知道您要去哪里，要他出这段跨国路由的费用，那可是贼贵贼贵啊，人家冤不冤啊。

这种收费的逻辑是基于成本而言的，现在只要被叫在归属地，就不对其收取费用，并不是说这段路由查询就不存在了，只要还是无线通信，路由的查询就是不可避免的。免除被叫的费用不是一种成本逻辑，而是一种商业逻辑。商业的逻辑也有点类似军事，那就是可以不计较一城一池的得失，追求的是一种整体的、宏观层面的胜利。被叫的费

用是免了，但企业在公众中美誉度的提高无疑也是一种弥补。

下面我们就来讲讲漫游费，首先从国际漫游开始，因为世界上大多数国家是不收取国内漫游费的，我国的国内漫游费的产生有其历史背景。

如图 6.17 所示，现在假如 A 国的移动台 MS1 漫游到 B 国，属于 A 国的另外一个移动台 MS2 对其进行呼叫。在路由到达移动交换关口局后向 HLR 进行查询得知移动台已经到达 B 国，于是将路由转至 B 国。

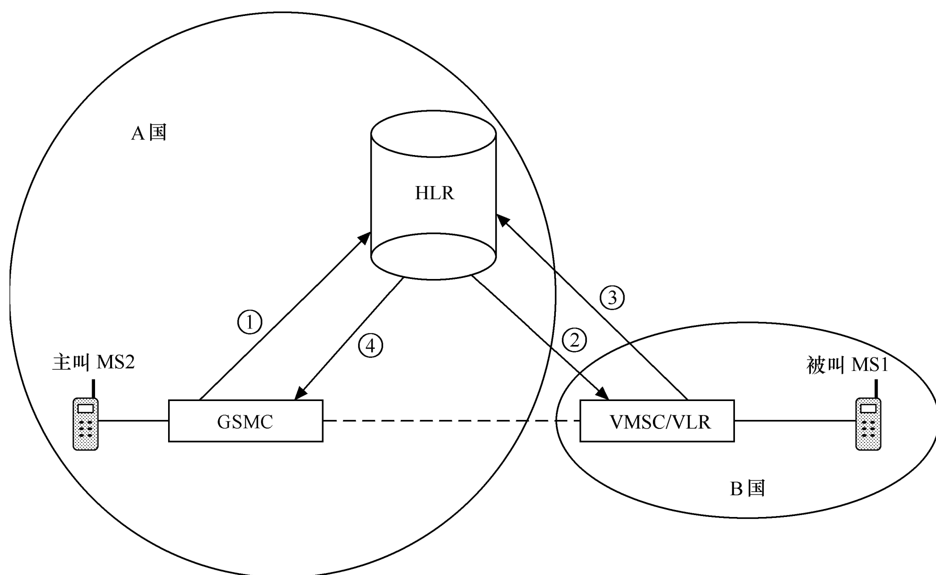


图 6.17　跨国漫游

原则上，主叫用户并不知道被叫用户的位置，主叫只支付原来应付的费用，也就是被叫移动台处于其归属 PLMN 时主叫应付的费用。也就是说，无论 MS1 是否出国漫游，主叫 MS2 只当 MS1 在国内，只支付这段路由的费用，而其余段的费用则由被叫承担。如果坚持所有费用都应该让主叫 MS2 出，那我们的技术体系就应该支持显示被叫 MS1 的所在位置，让主叫 MS2 自行决定是否应该拨打。应当说谁也不希望自己在什么位置被别人知道得清清楚楚吧，所以被叫的位置只有 HLR 知道，是不公开给主叫的，这称为移动台的位置保密原则，为此被叫付出的代价是必须承担相应的费用。

这里有两家 PLMN 网参与了整个通信的过程，即 A 国的 PLMN 网和 B 国的 PLMN 网，这两者之间是有一条国际线路的，A 国的 PLMN 网是要支付这一段长途费用的，如果在图 6.17 那段虚线有中介的通信网，那么该中介网也可以分享这段费用。

知道了国际漫游费的计费机理我们就来谈谈国内的。

20 世纪 90 年代中期，我国移动通信事业刚刚起步，全国手机用户不到 1000 万，而



且东部地区无论在网络资源、用户数量和资费竞争上都明显优于中西部地区，考虑到这种不平衡性，当时就提出了收取国内手机漫游通话费。

举个例子说明一下。西部地区的消费者和用户，去买东部地区如北京、上海、江苏的号，然后到西部地区去使用。这样的话，等于是使用了西部地区的网络，但是收入是归东部地区的企业，如此就会加剧我国移动通信事业发展的不平衡。所以咱们就建立了一个门槛，倘若离开你手机号注册的当地，费用要提高，这样的话就不会有西部地区的用户来买东部地区的手机号了。

时到如今，三大运营商逐渐形成了全程全网，全国一盘棋的格局，当年担心的因素，即西部网络的发展会因此而放缓已经慢慢消于无形。但是按原先的规矩漫游费在各省之间是要进行结算的，归属地分一部分，漫游地又要分一部分，这就形成了各省运营商之间的利益格局。漫游资费的调整与各省运营商的切身利益息息相关，而中国经济在东部与中西部的发展又如此不平衡，导致了中西部大量劳动力涌向东南部打工或经商或寻找机会，东南部运营商的 MSC 里漫游用户那是大把大把的，这些用户占用了当地的有线和无线资源，而资费却是由归属地的运营商收取，这其中的利益无疑要在归属地和所在地的运营商之间进行分割，这种历史和社会现实形成的利益格局一时之间确实也难以消弭。

从技术上而言，国内的漫游与跨国漫游在这个层面上也没有什么本质的区别，包括 A 地 PLMN 网与 B 地 PLMN 网之间的漫游费的结算与国际漫游的惯例也没有本质的区别，不过就是国与国之间的 PLMN 网改成了归属地与非归属地之间的 PLMN 网而已（如图 6.18 所示）。

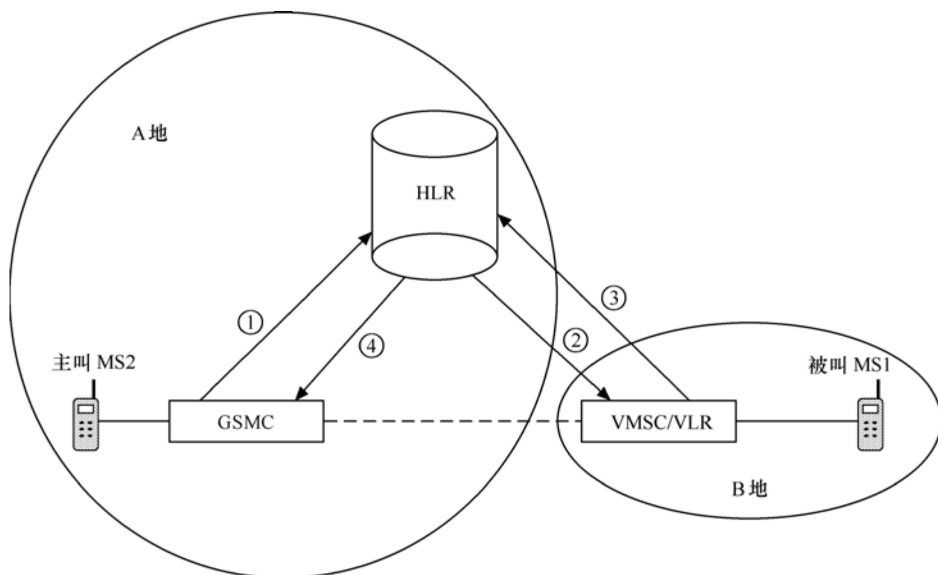


图 6.18　国内的漫游

第7章

Chapter 7



要把文章写好，先要学好语法——也谈七号信令

学习第 6 章第三层协议和本章七号信令的目的都是一样的——为学习信令流程打基础。信令流程可以让我们明白一个真正的商业无线通信系统究竟是怎样运作的。学习信令流程之前，我们得先把信令中最难的两部分挑出来成为两章，好让大家对此有深刻的认识，至于其他部分的信令，我们可以留待第 8 章再讨论。另外，Um 接口的第三层协议和 A 口的七号信令也是平时进行信令分析用得最多的两个接口，至于 Abis 接口的信令，我们有必要做一定的了解，不过由于 GSM 规范对这个接口没有作详细严格的规定，各厂家往往自己有自己的实现方式，因此在这个接口花过多笔墨意义并不大。

图 7.1 所示为常见的 GSM 协议一览图，我们分别用圈标注了第 6 章和第 7 章关注的内容，到了第 8 章，我们需要把前面所有的知识串连起来，对整个 GSM 无线通信网络有一个系统的认识。

谈到七号信令，本章还是打算先跳到技术的视野之外，从流水线和产业链的思维角度来介绍 OSI 七层模型。七号信令与 OSI 七层模型有类似的分层结构，由于由马萨诸塞大学的 James F.Kurose 与纽约理工大学的 Keith W.ROSS 合著的《Computer Networking A Top-Down Approach》一书的问世，对于这类分层结构的分析通常是自顶向下的。但是在本书中，作者依然打算采用传统的自底向上的方式来对这些问题进行阐述。James F.Kurose 之所以对网络进行自顶向下的分析，是因为互联网应用层的内容，无论是 FTP、HTTP 还是 DNS、E-mail，大家都已经很熟悉而且对其工作原理饶有兴趣，而七号信令的应用层比如 TUP、ISUP、MAP、BSSAP 对于绝大多数人来说根本就一点都不熟悉，直接从顶层讲起效果恐怕适得其反。



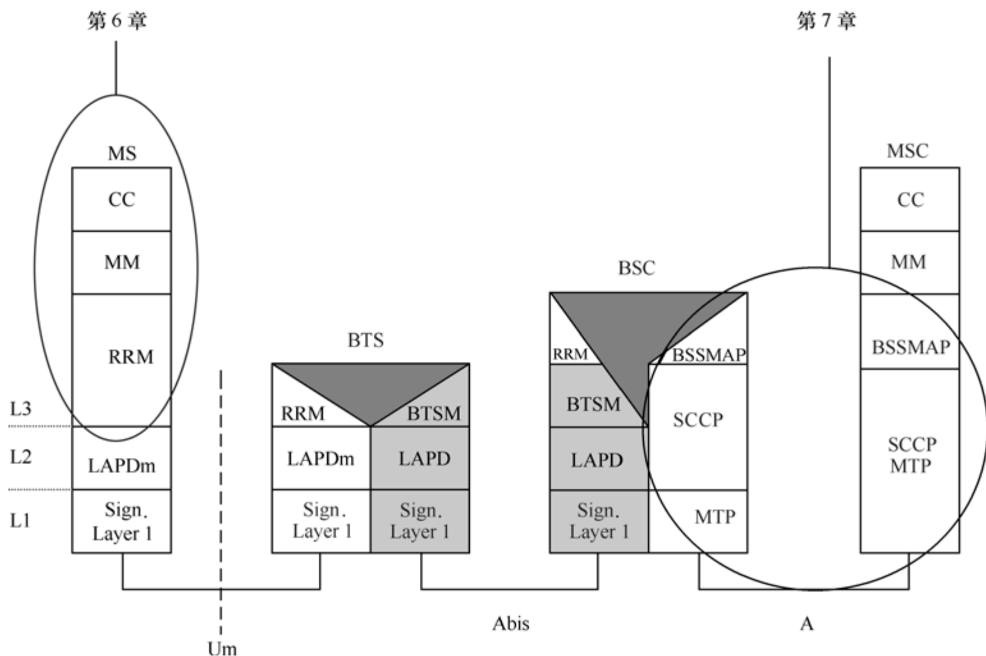


图 7.1　第 6 章和第 7 章关注的内容

虽然采用了传统的分析方法，却未必要采用传统的表述方法，作者试图用故事的方式使本章尽量轻松化一点，因为七号信令的学习从来就是一个枯燥的活，作者不想大家一翻到本章就上下眼皮不停打架，呵呵。

7.1 信令的基础

在谈七号信令之前，我们先来看看什么叫信令。人有四肢，可是它们要活动还需要大脑给指令；人有五官，可是离开神经它们毫无用处，有人失去了嗅觉，有人失去了听觉，很多时候并不是五官本身损坏了，而是控制它们的神经受到了损伤。通信系统的控制指令就称为信令，通信网的神经系统就是信令网。

通信时线路上会跑很多信息，除了用户的语音信息和数据信息以外的控制交换机动作的信号，就是信令。

7.1.1 研究信令的手段——分类

信令是有几种不同的分类方式的，分类是一种学习知识和进行研究的有效的手段。我们一看欧美人，觉得他们都是从一个模子里刻出来的，谁和谁都长得差不多，行为举止神

态差不多，不好区分，那是因为我们的分类标准没有建立起来，我们认识起中国人来就要简单得多，你的同学、朋友、同事、邻居，你在电视上认识的演员明星或者其他人，加起来得有几千个吧，没看见你把谁跟谁弄混。我们之所以认为中国人好认是因为我们长期生活在这片土地上，已经潜移默化地形成了一套辨识标准，尽管你没有办法讲清楚你用于区分判别的标准体系。地理环境会给人的生理特征打上烙印，你可以清楚地分辨来自陕北或者来自水乡的人；人文环境会给人带来不同的气质，上海人和北京人是截然不同的；家庭熏陶会让人产生不同的思维方式，书香门第和商贾之家的人的行为方式也是不同的。

杂七杂八讲了这么多，无非想说明，要想对事物有清晰的认识，通过分类来提高事物彼此之间的辨识度是一个不错的办法，我们下面就来对信令分分类。

1. 随路信令和共路信令

这是按传送信令的通道来进行划分的。起初，信令是和话音一起传送的，后来随着通信网的发展，这样做的局限性逐渐暴露了，这才有了共路信令，就是单独划一条通道给信令用。这与我们的城市交通也颇有相似之处，我们一些大城市的城市道路，早先也是所有汽车混着跑的，跑着跑着就发现这样对城市交通而言效率太低了，公交车（信令）开得太慢了，于是很多城市就划了一条公交专用通道，这条道只允许公交跑，这与共路信令系统实有异曲同工之妙。

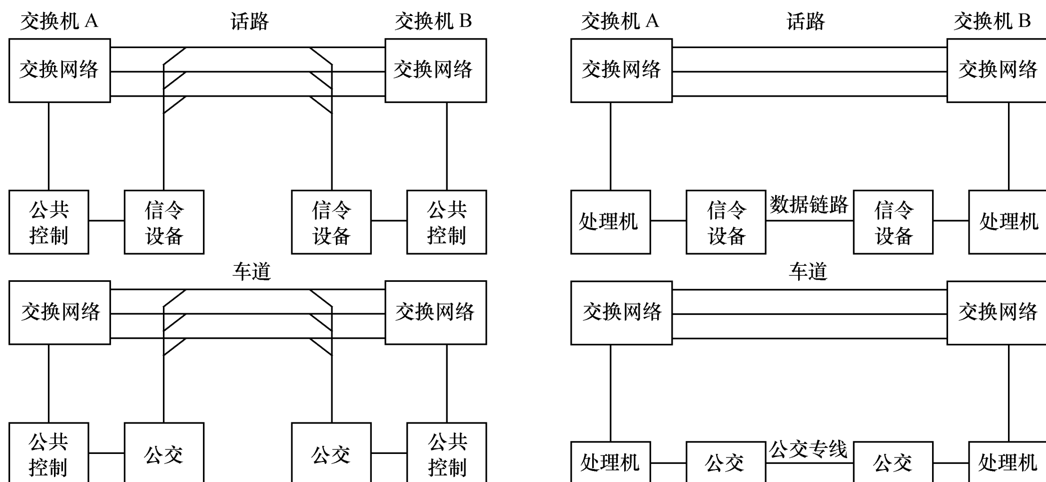


图 7.2　随路信令、共路信令与公交网络

由图 7.2 可知，随路信令系统两端的交换机的信令设备之间没有直接相连的信令通道，信令是通过话路来传送的。当有呼叫到来时，先在选好的空闲话路中传递信令，接续建立后，再在该话路中传送语音。随路信令的信令通道和用户通道合在一起。



共路信令系统两交换局的信令设备之间有一条直接相连的信令通道，信令的传送是与话务分开的、无关的。当有呼叫到来时，先在专门的信令通道中传信令，接续建立后，再在选好的空闲话路中传语音。因此，共路信令也称公共信道信令。

我们看到了，是随路信令也好，是共路信令也罢，都得信令先行完成接续才开始进行语音的传送。就好比一支军队一样，旗未动，鼓未敲，你就乱跑，那是要杀头的！

2. 线路信令、路由信令和管理信令

信令按其功能可分为线路信令、路由信令和管理信令，就好比交通局有三个岗位的工作人员（监察员、调度员、交警）一样。

监察员的工作是守在监控室查看各个车辆的状况，如哪里有违章，哪里有超速，哪台车又熄火了，哪台车又重新启动了。线路信令是具有监视功能的信令，用来监视主、被叫的摘挂机状态及设备忙闲。

调度员算是交通局开发的增值业务了，路这么多，司机搞不清该怎么走，调度员负责给司机正确的路由指向。路由信令是具有选择功能的信令，它通常通过分析被叫号码来选择合适的路由。

交警是搞管理工作的，哪里出车祸了，路堵了，在路口竖一块“前方有事请绕行”的牌子，疏导车辆走别的路，路况恢复正常的时候又把牌子撤掉，让车子过来。管理信令是具有操作功能的信令，用于电话网的维护和管理，如检测和传递网络拥塞信息，提供呼叫计费信息，提供远距离维护信令等。

3. 用户线信令和局间信令

信令按其工作区域不同可分为用户线信令和局间信令。

用户线信令是用户和交换机之间的信令。比如说交换机给用户发送的铃声和忙音，以及用户向交换机发送的主/被叫摘挂机信令都属于用户线信令。由于每一条用户线都要配一套用户线信令设备，所以用户线信令应尽量简单，以减少用户设备的复杂程度，从而降低成本。

局间信令是交换机和交换机之间的信令，在局间中继线上传送，用来控制呼叫接续和拆线。局间信令是比较多和复杂的，因为要满足交换机互相对话的要求。

7.1.2　从结构形式到控制方式——信令的剖析

信令可以从结构形式、传送方式和控制方式来进行剖析。

1. 结构形式

信令的结构形式分为未编码和已编码两种。对于未编码的脉冲信号，目前已经不用

了；已编码信号中，又分为以下三种信令：

① 模拟已编码信令：分为起止式单频二进制信令、双频二进制编码信令及多频制信令，其中使用的最多的是六中取二的多频信令，它设置 6 个频率，每次取出 2 个同时发出，表示一种信令，共可表示 15 种信令。中国一号记发器信令使用的就是多频信令；

② 数字型线路信令是使用 4bit 二进制编码表示线路状态的信令；

③ 七号信令是使用经二进制编码的若干个八位位组构成的信令单元来表示各种信令。这是本章的重点内容。

2. 传送方式

人和人之间开始是并不认识的，一个人想结识另一个人，往往需要中间人来递话。与此相似，发端局和收端局之间往往不是直接相连的，之间往往有一个或者几个转接局，那么就必定要涉及信令如何在多段路由上传送的问题，传送的方式一般有如下 3 种：

（1）端到端方式

如图 7.3 所示，发端局的收码器收到用户发来的全部号码后，由发端发码器发送转接局所需要的长途区号（图中为 ABCD），并将电话接续到第一转接局，告诉它，俺要找某某某局（ABCD），具体要找的人不告诉它；第一转接局根据收到的 ABCD，一瞅："嗨，要找的不是咱，这个局咱也不知道门路，高攀不上啊，不过，我介绍给你一个朋友，它离你要找的近点"，于是给发端局做了个介绍，把电话接续到第二转接局；发端局又拜访第二转接局，告知来意："俺要找 ABCD 局"，第二转接局跟收端局是老交情了，就把电话接续到收端局。如此这般发端局终于找到了收端局，一番拜访寒暄之后发端局把详细的电话号码告诉收端局："俺要找你局的×××××××"，收端局接续被叫，这样就完成了主叫和被叫的接续。

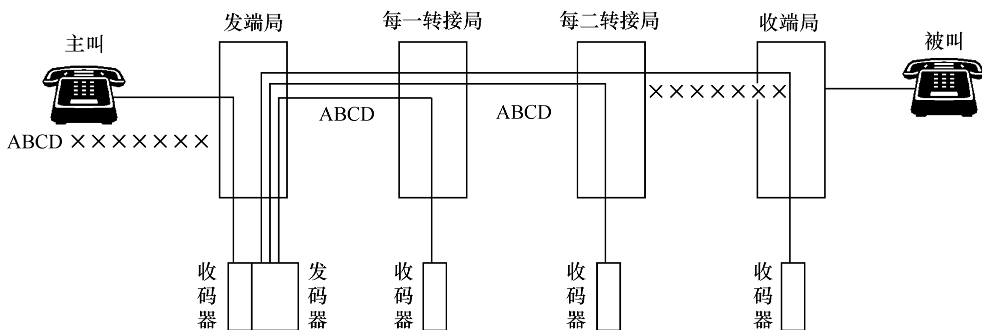


图 7.3　端到端的方式



端到端方式的特点是：速度快，拨号后等待时间短。速度快是相对我们接下来要讲的逐段转发方式而言的，这很好理解，去衙门办事，当然是事必躬亲比较快。

（2）逐段转发方式

如图 7.4 所示，信令逐段进行接收和转发，全部被叫号码（ABCD×××××××）由每一个转接局全部接收，并逐段转发出去。

恩，不是什么衙门都态度好，肯一级级指点你找到相应的人。人家直接跟你说："把啥资料都扔这儿吧，我们到时候帮你转达"。噻，你不能直接去找要找的人，当然不能只告诉人家所在的局（ABCD）了，一定要把详细的信息告诉人家（ABCD×××××××）。

逐段转发方式的特点是：对线路要求低；信令在多段路由上的类型可以多种多样；信令传送速度慢，接续时间长。

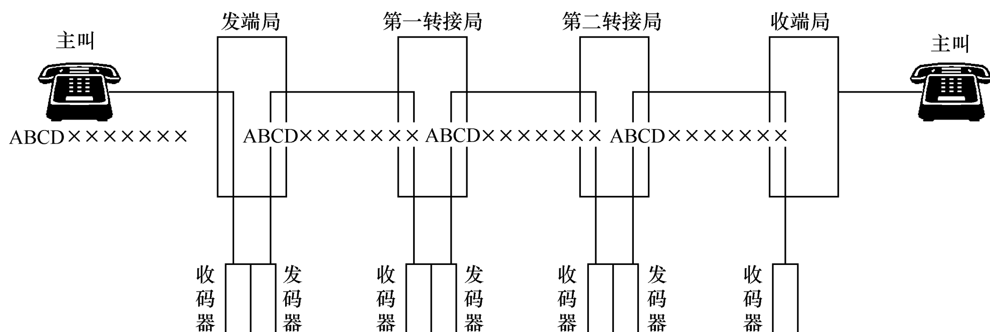


图 7.4　逐段转发方式

（3）混合方式

在实际中，通常将端到端方式和逐段转发方式结合起来使用，这就是混合方式。如中国一号记发器信令可根据线路质量，在劣质电路中使用逐段转发方式，在优质电路中使用端到端方式；七号信令通常采用逐段转发方式，但也可提供端到端信令。

3. 控制方式

这个传送信令很多情况下就像搞访谈节目，一般情况下都是有问有答，有来有回的。你说的话对方得有回馈才表明他听到了，无论是语言也好，眼神也好，动作也好，总之得有回馈；如果你说得太快，或者说得让对方不明白，对方就会打断你，请你重复一遍。

我们这里所说的控制方式是指控制信令发送过程的方法，包括以下 3 种方式。

（1）非互控方式（脉冲方式）

如图 7.5 所示，非互控方式即发端不断地将需要发送的连续或脉冲信令发向收端，

而不管收端是否收到。这种方式设备简单，但可靠性差。

这种有发无收的信令传递模式都有点不像对话了，更像泼妇骂街，呵呵。

（2）半互控方式

如图 7.6 所示，发端向收端每发一个或一组脉冲信令后，必须等待收到收端回送的接收正常的证实信令后，才能接着发下一个指令。

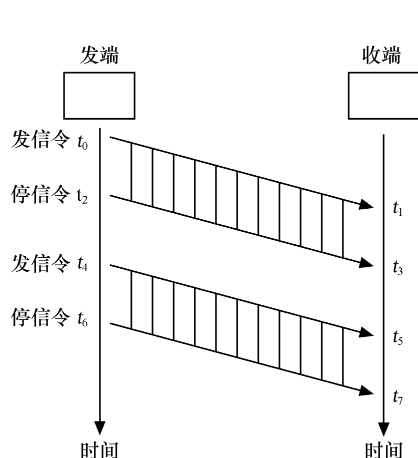


图 7.5　非互控方式

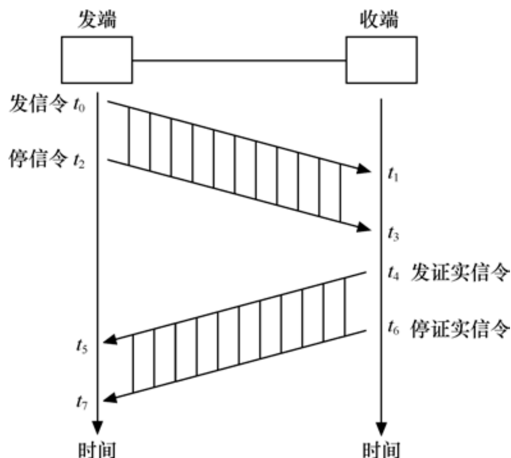


图 7.6　半互控方式

由发端发向收端的信令叫前向信令，由收端发向发端的信令叫后向信令。半互控方式就是前向信令受后向信令控制。

半互控方式很像你教一个刚刚入门的学生英语，你教英语叫做前向信令，学生学着读英语叫做后向信令。你教一句就得停下来，等着对方反馈，看对方是否明白了，要不等学生反馈就开始下一句学生是跟不上的，所以你的教学速度实际上受制于学生的反馈速度，这叫前向指令受后向指令控制。

（3）全互控方式

全互控方式有点特别，发端发前向信令不能自动中断，要等收到收端的证实信令后，才停止发送；收端发证实信令也不能自动中断，须在发端信令停发后，才能停发证实信令。因为前向信令和后向信令均为连续的，所以称之为连续互控。这种方式抗干扰能力强，但是设备很复杂。

如图 7.7 所示，全互控方式很有点类似记者做访问类节目，嘉宾在不停地说话（发信令 t_0），记者边记边点头回馈嘉宾，意思就是俺记下啦（发证实信令 t_2）。嘉宾收到反馈，觉得记者 MM 记得太辛苦啦，于是说“我这一句说完了”（停信令 t_4）。记者 MM 趁这时间记好笔记，然后说“了解”（发证实信令 t_6），这时候嘉宾开始说第二句（发信令 t_8）。



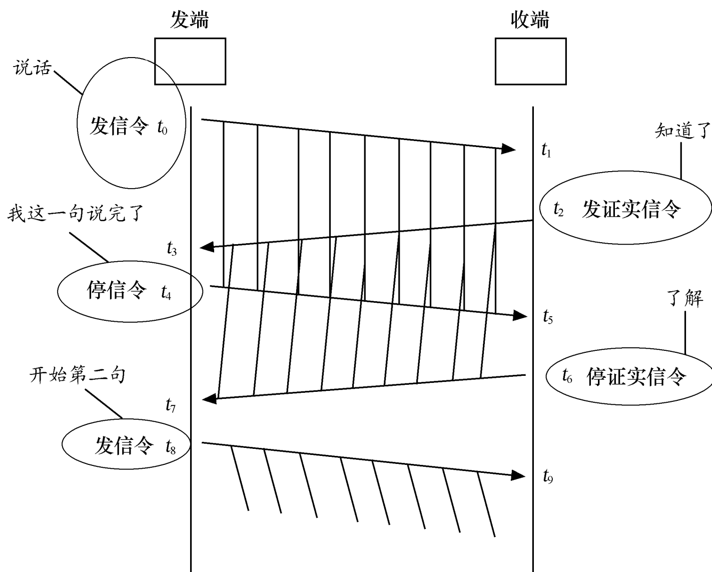


图 7.7　全互控方式

7.2　从流水线和产业链说起——也谈OSI七层模型与七号信令

现代社会呈现出如此生机勃勃的繁荣景象某种程度上应该感谢科学管理之父弗雷德里克·温斯洛·泰勒。泰勒的科学管理理念的精髓之一就是进行流水作业，把一个工作拆分为若干个环节，每个环节都实行标准化，确定操作规程和动作规范。工作的分解和劳动过程的标准化，使得原来复杂的工作通过分解和重复变得简单了许多，从而大大提高了劳动生产率。

泰勒的思想不仅深深地影响了制造业，而且逐渐发散到各个行业。近 20 年以来，流水线生产方式被深刻理解，各行各业都争相引入流水线生产方式。以软件开发为例，20 年前做软件开发，就是程序员单枪匹马去编码、编译和调试。随着软件工程得以应用，软件开发细化为架构设计、软件编码和测试等几个部分，软件开发可以采用工厂化的流水线生产方式来进行。用流水线方式生产软件与软件工程师单打独斗编程相比，能够发挥规模经济的优势，使得软件开发成本大幅度下降。

上文中我们左一个泰勒，右一个泰勒，泰勒与 OSI 模型到底有什么关系，泰勒时代还没有计算机和现代通信吧？把他跟麦克斯韦、马可尼、贝尔、史端乔放到一起，想说明什么呢？别急，我们先来看看一个合格的通信系统应该做些什么。

贝尔发明了电话，史端乔发明了交换机，电话加交换机合在一起就可以组成一个通信网络了。然而光有物理设备还不够，得发明一整套指挥系统来控制这些设备本身以及

上面跑来跑去的比特流，才能完成正常的通信。就好比古代乌压压十万大军，矛尖盾厚、车甲齐备、粮草充足，但没有旌旗金鼓，没有律令条例，指挥和控制系统没建立起来，那就是一群乌合之众，是打不了仗的。

在通信网络中，这个指挥系统的指令称之为“信令”，GSM 系统中 A 接口传输的信令，我们称之为七号信令。七号信令采取了和 OSI 七层模型非常相似的结构。

这个七号信令应该完成一些什么工作呢。不管怎样，要传递信令首先得有通路，就像开汽车得先有马路一样，你得定义这条通路的物理、电气功能特性和链路接入方法；除此之外，道路通了，你是不是得保证一端到另一端信号可靠的传输，不能丢，不能错，不能以次充好，就是运送货物，这也是基本的条件吧；俗话说条条道路通罗马，然而到底该选哪条路，那是乱花渐欲迷人眼，看都看不清楚，到底选哪条路好得有个负责选路的人吧；传递信号的应用层软件是很多的，就如需要运输货物的客户也是很多的，从电脑到水果林林总总，不一而足……

传递一个信令要干的事情这么多，如果要让一个研究人员从头管到尾，累死他也做不到。要完成这些工作，我们得学习泰勒的科学管理法（这不是来了），挥舞起大剪刀，咔嚓咔嚓咔嚓咔嚓，把这些事情剪成七块，这个叫分层，也就是分工；光有分工也不行，每一层对另一层而言必须像一个黑盒子一样，不管你盒子里面怎么折腾，我从外面看都是一样的，我只需要在你的黑盒子上再叠加我的黑盒子就够了，用比较专业一点的话说是，每一层设计东西的变化不能影响其他的层级，你物理层的东西的变化不能影响我应用层，就好比你把 INTEL 的 CPU 换成 AMD 的，我这腾讯 QQ 不能就跟着得重新设计，要不大家就没法混了。

分工的重要性大家应该都明白，没有分工就无所谓专业，没有专业就无所谓效率。但是这层级与层级之间的工作应当怎样设计才能使每一层的变动都不会对其他层次构成影响，这个或许一时之间难以理解深入。我们不妨先从技术层面之外的东西来了解一下，不是说泰勒思想已经深入各行各业了么，我们来看看一个典型的分层结构——苹果公司的 ipod 的产业链是怎么做的。

如图 7.8 所示，我们看到，产业链各层级的分工非常清晰，从研发到销售各司其职，如果你让搞研发的还去琢磨这个 ipod 零件如何生产，该怎么组装，去哪里卖，这个研发工作能搞好才见鬼了。问题是产业链不是光分工明晰就可以的。一定要标准化，一个解码器，无论是东芝还是三星亦或飞利浦，生产出来的必须完全符合同样的标准，

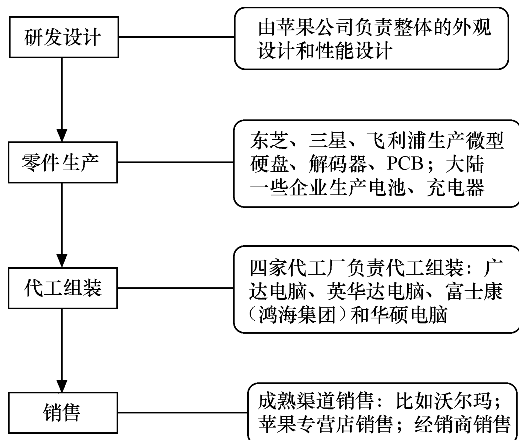


图 7.8　ipod 产业链分工



要不一堆千奇百怪的零件最后交到富士康或华硕的手里组装出来一定变得更加千奇百怪。

好的，解剖了 ipod 的产业链之后，我们得把自己通信这块要完成的工作也解剖解剖了。要想富，先修路，要想通信，也得先修路，定义这条路的标准，这是物理层的工作；人生不如意常八九，路上打劫者常五六，要保障信号从路的这一头完整地走到那一头，不出错不少东西不被调包，这可不是一件容易的事，这件苦差事交给数据链路层来做，这位老兄，你就“把信送给加西亚”好了；如果说以上两项是苦力活，下面要说的就是智力活了，哪条路最近，哪条路没堵，哪条路重新又通了，对这些信息的管理与调度是网络层要干的活；基于这三层上面的传输层、会话层、表示层跟咱本章的工作没有多少关系，就不在这里啰唆了；最后就是应用层了，话说这又是修路，又是防打劫防货物丢失，又是画拓扑图找路由好省点油钱的，都是为谁辛苦为谁忙啊，还不是为了您应用层呗，在通信系统中，应用层可啥内容都有，什么 TUP、ISUP、BSSAP 的，就如搞个物流的谁都找你门上来了，寄个信，发个礼物，托运电脑，都是业务啊，只要赚钱的活，咱通通都干，怪不得应用层越来越膨胀了，搞得唐僧还专门设了一个部门经理，这都是后话，咱们稍后再议。这一级级功能是划清楚了，标准也是清楚了。比如第二层，那活就是要“把信送给加西亚”，你就是不能搞错不能搞漏了，更不能因为工作忙就要第三层给你分担压力，你第二层就是干苦力活的，俺第三层就是搞调度搞管理的，按孔子的话说，就是“上智下愚不移”，随便更改工作标准，工作性质是会引起混乱的。

我们在这里画出 OSI 七层模型的图（如图 7.9 所示），中间的那三层反正七号信令不用，TCP/IP 也不用，我们就将就看看，不让它搅活到我们的“物流模型”里面去了。

说明	层
第 7 层：直接对应用程序提供服务，应用程序可以变化，但要包括电子消息传输	Application 应用层
第 6 层：格式化数据，以便为应用程序提供通用接口，这可以包括加密服务	Presentation 表示层
第 5 层：在两个节点之间建立端连接。此服务包括建立连接是以全双工还是以半双工的方式进行设置，尽管可以在层 4 中处理双工方式	Session 会话层
第 4 层：常规数据递送——面向连接或无连接。包括全双工或半双工、流控制和错误恢复服务	Transport 传输层
第 3 层：本层通过寻址来建立两个节点之间的连接，它包括通过互联网络来路由和中继数据	Network 网络层
第 2 层：在此层将数据分帧，并处理流控制。本层指定拓扑结构并提供硬件寻址	Data Link 数据链路层
第 1 层：原始比特流的传输，电子信号传输和硬件接口	Physical 物理层

图 7.9　OSI 七层模型

七号信令的基本功能结构由消息传递部分（MTP）和用户部分（UP）组成。UP 可以是电话用户部分（TUP）、数据用户部分（DUP）、ISDN 部分（ISUP）等，具体的应用还有很多，我们就不一一详细列举了。

图 7.10 所示只是七号信令的简单结构，消息传递部分（Message Transfer Part，MTP）就包含了 OSI 模型一至三层的功能，我们需要继续进行细分。

说起来，七号信令的模型与 OSI 基本一致，不过和 TCP/IP 一样，七号信令也只有四层，依次称为信令数据链路级 MTP-1（对应 OSI 七层模型的物理层），信令链路控制级 MTP-2（对应 OSI 七层模型的数据链路层），信令网功能级 MTP-3（对应 OSI 七层模型的网络层），用户级（对应 OSI 七层模型的应用层），我们画出两个信令点通信的示意图如图 7.11 所示。

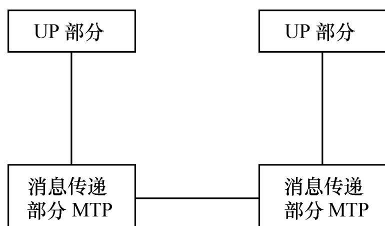


图 7.10　七号信令基本功能结构

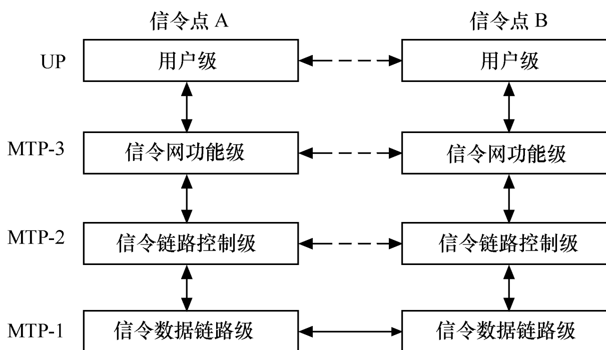


图 7.11　七号信令系统的四级结构

其中各层的功能如下。

MTP-1：为信令传输提供一条双向数据通道，定义了信令数据链路的物理、电气功能特性和链路接入方法。

MTP-2：定义了在信令数据链路上传送信令消息的功能和程序。它和第一级一起共同保证信令消息在两信令点之间的链路上可靠地传送。

MTP-3：在消息的实际传递中，将信令消息传至适当的信令链路或用户部分；当遇到故障或拥塞时，完成信令网的重新组合，以保证信令消息仍能可靠地传递。

UP（User Part）：由各种不同的用户部分组成，每个用户部分定义和某一类用户相关的信令功能和过程。

我们这里的用户与大家通常意义上理解的用户是不一样的，指的是消息传递部分 MTP 的用户，比如 TUP、ISUP 之类，你不妨把 E-MAIL、FTP、HTTP 也理解为 TCP-IP 的用户。

应当说我们上面的七号信令各层的结构还很初级，很不完善，比如说 MTP-3 利用 DPC



进行寻址，而 DPC 的编码只在一个信令网内有效，不能跨网进行直接寻址；另外，MTP-3 不能完成段对端的信令传输，如果中间有信令转接点，只能采取逐段转发模式，再者 MTP-3 识别用户的 SI 只有 4bit，导致一共只能支持 16 个用户，远远不能满足现代通信发展的需求。对于以上细节问题我们会在后面几节中详细讨论，我们现在只要知道由于这些问题我们又增加了 SCCP 和 TCAP，就形成了目前的七号信令系统（如图 7.12 所示）。

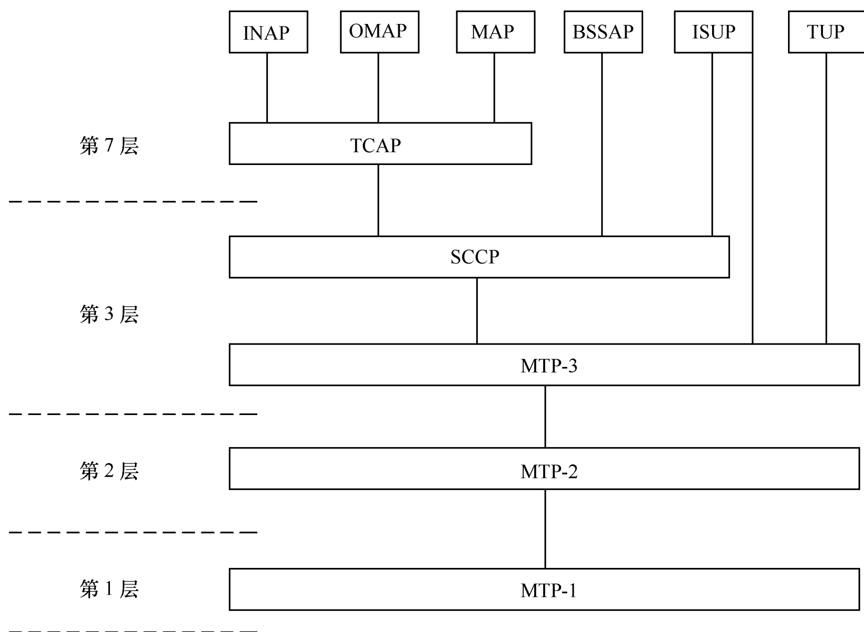


图 7.12　七号信令功能级结构

我们对七号信令有了整体的初步的概念，下面的章节我们就要来一层层对它们进行分析。

7.3 唐僧开物流公司——也谈MTP-1 和MTP-2

话说唐僧西天取经后，虽然被封了个旃檀功德佛，但是在西天一直得不到重用。眼看现在市场经济时代，众神下海的下海，经商的经商，个个赚得那是盆满钵满。三藏兄终于忍不住了：“俺当年步行十万八千里，经过九九八十一难，不就图来西天享个清福么。结果俺这个一心向佛的过得如此郁闷，那帮酒肉之徒倒是潇洒快活，罢罢罢，形势比人强，市场经济时代，不会挣钱的佛不是好佛，俺还是回俺的东土大唐一趟，挣点外快去。”

主意拿定，三藏遂向如来告了个假，投奔大唐的结拜老兄唐太宗李世民去了。唐太

宗见是御弟来了，自是热情招待，酒过三巡，三藏遂向李世民吐露了心中苦恼。太宗听罢，颔首微微一笑："御弟，此事有何难哉，现在不是物流很赚钱吗。你就在大唐做物流吧，朕批准你在长安—虎牢关—洛阳一线做物流，等做大了朕再批别的路线"。

三藏一听大喜，这可是大唐最肥的一条路线啊，于是拜谢过太宗，急匆匆寻找昔日部下组建公司去了。

7.3.1　白龙马的世界级企业梦想——信令数据链路级 MTP-1

要搞物流，先得修路，这没办法，大唐当年的运输条件就这样。三藏遂找来当年的白龙马同志共商大事，白龙马是个老司机了，驮着唐僧走了那可是十万八千里啊，这路该怎么修，他最有发言权了。

白龙马知道师傅与世民哥哥的交情，知道赚大钱的机会来了，乐得屁颠屁颠地就来给唐僧出主意了："话说师傅啊，这路咱不用自己修，让陛下发道诏书，征集上万百姓就可以了。不过咱得制定标准，都说一流的企业做标准嘛。咱们这条路的标准称为信令数据链路级标准，也称 MTP-1 标准。你不是说以后要在这条路上跑七号信令么，那咱的标准就是：得采用 2M 线的 TS0 以外的时隙来传递信令，信令的速率为 64kbit/s，这个就称之为 MTP-1，也就是那个什么 OSI 常常说的物理层"。

"晕，你这标准也太简单了吧，就这也能申请专利，咱就靠这去做世界一流的企业？"唐僧只觉得眼冒金星，小白龙顿时无语凝噎。

7.3.2　任劳任怨的沙和尚——信令链路控制级 MTP-2

唐僧在家里生了几天闷气，这时候太白金星前来拜访了。太白金星听完三藏的抱负和白龙马的点子之后哈哈一笑："我说旃檀功德佛，亏你行程十万八千里，历经九九八十一难，眼界还是不够高啊，看得还是不够远啊，这才哪到哪呢。一个 OSI 有七重境界，你这才刚练到第一层呢，不要嫌第一层太简单，七层都能像这样码得牢牢实实，你这个企业可是蔚为壮观啊，不比世界一流企业差的"。

唐僧听到这里又高兴了起来，这路修好了，做物流的话下一步该找组织运输工了。话说这运输大队长一职，唐僧最钟意沙悟净了。悟净自东土到天竺，一路上勤勤恳恳挑担子，无论是工作态度还是执行力都没得挑，经验也十分丰富，这"把信送给加西亚"的活，非沙和尚莫属了。

话说沙僧在如来身边当金身罗汉，实际上也就是如来的贴身保镖。如来法力无边，没有人敢打劫，所以秉承着少劳少得的原则，沙僧挣得也并不多。一听师傅这里开公司了，还可以分原始股，沙僧自然乐得投奔过来。

沙僧接到的第一笔单子来自 ITM 公司，说是要传递什么比特流，比特流说简单也简

单，就两种型号，一种叫做“0”，另一种叫做“1”。沙僧一听就乐了，这么一笔大单就这么简单的工作，那还不是小菜一碟，挣钱也太容易了。结果仔细一看合同条文傻了眼，这 ITM 公司可够苛刻的，这些比特流 8 个一组，若干个组称为一个信令单元，每个信令单元最少有 6 个八位位组。ITM 要求比特的顺序不能乱，而且一个都不能错，错了就得重新发一组，因为 ITM 公司说每个组顺序不同了也好，0 信号变成了 1 信号也罢，都代表不同的意思，所以这是绝对不能错的（七号信令中 8 个 bit 算作一组）。

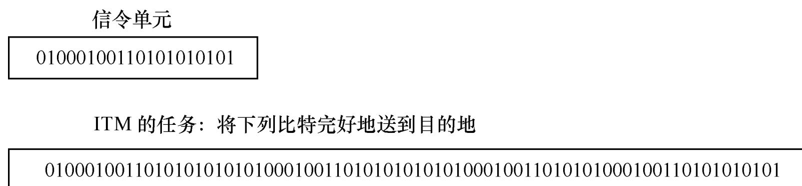


图 7.13　ITM 的信令单元和任务

沙僧不知道怎么办，拿来问师傅。唐僧半闭着眼睛念念有词：“啥叫‘没有任何借口’、啥叫‘把信送给加西亚’，啥叫‘执行力’啊。这都搞不定要你这运输大队长作甚？”沙僧知难告退，只得自己想主意。

沙僧知道，要将这一串比特流完好地送到目的地首先要保证的是每个信令单元信号的正确性，信令单元的信息要是乱了，也就等于整个比特流的信息乱了，俺先从小处着手。

1. 定界

沙僧翻阅了 ITM 送过来的技术资料，资料上说信令单元一共有 3 种形式：消息信令单元（Message Signal Unit，MSU）、链路状态信令单元（Link Status Signal Unit，LSSU）、插入信令单元（Fill-In Signal Unit，FISU），姑且不论这些信令单元是做什么用的，光其中一点特性就够要命了，这些信令单元有的 128bit，有的 256bit，它们不等长！不等长有什么要命的地方？请问图 7.14 所示的比特流到底可以划为几个信令单元？请问有谁知道呢？

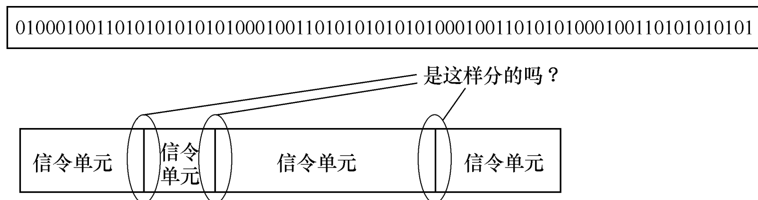


图 7.14　比特流如何分解成信令单元？

沙僧决定完成第一步工作，就是怎么也得把信令单元与信令单元之间的界限区分出来，这个工作称之为“定界”。

什么叫定界？定界就是采用码型为“01111110”的标志码作为信令单元的分界，它既表示上一信令单元的结束，又表示下一信令单元的开始。（请注意，为了践行七号信令中所有符号都为 8 位位组的理念，俺的定界码也是 8bit 的）这个标志码也称为“F 字段”。

那么比特流就变成了如图 7.15 所示。

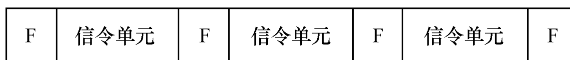


图 7.15　信令单元的定界

定界的问题到这里并不算都解决了，假如信令单元里本身就有个“01111110”的码型那可咋办呢？这问题不难，就好比你个隋朝人到了大唐偏偏又有个“世民”的名字，那该咋办，为忌天子讳把你的名给改了。

对付这种企图鱼目混珠冒充定界码的刁民的办法就是在信令的发送端进行“0”比特插入，在接收端进行“0”比特删除。

所谓“0”比特插入，就是在发端连续发 5 个“1”之后插入一个比特“0”，不让你搞成连续 6 个 1 避免和我们的标志码搞混。到了接收端，把这个插入的“0”去掉就是“0”比特删除。

在实际操作中，定界的功能是由硬件电路自动完成的。

2. 信令单元定位

如图 7.16 所示，我们刚刚完成定界工作，规定了除了标志码以外，不得出现连续 6 个“1”的码型，如果出现了这种情况，说明信令信息出错了。另外，我们说了，信令单元都是由 8 位位组构成的，而且最少都有 6 个 8 位位组，最多也不能多于 m+7 个 8 位位组（m=62 或 272），如果出现了信令消息比特个数不是 8 的整数倍或者位组小于 6 个大于 m+7 个的情况，说明链路出错了，我们称之为“失去定位”，从而进入信令单元出错率监视过程，也就是我们本节第 7 部分的内容。

3. 误差检测

话说 ITM 的条件虽然很苛刻，但也不是一个比特不许错。对于七号信令消息，一般要求误码率低于 1.2×10^{-6}。悟净狂晕：“这与一个也不许错有啥区别”。当然，既然提出了误码率的要求，那首先得增加一个检验机制，查查到底比特流是否有出错。

悟净决定将信息单元的所有比特对一个生成多项式 G（x）做一个除法运算，得出一个 16 比特的余数 $r(x)$，取其二进制反码附在这些信息位的后面，称为 CK 字段（如图 7.17 所示）。



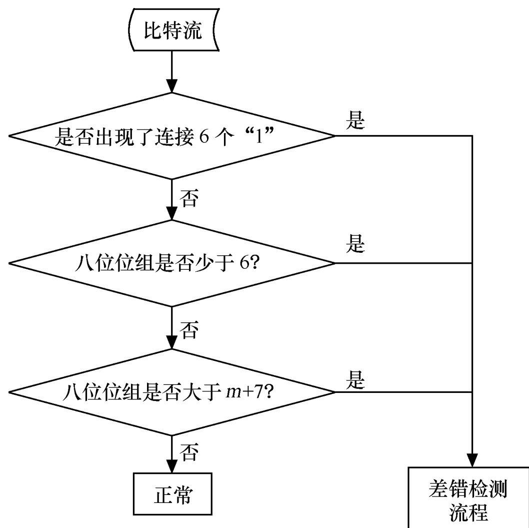


图 7.16　信令单元定位

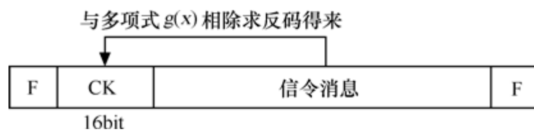


图 7.17　循环码校验法

这样就相当于生成了一个多项式，该多项式 $T(x)=x^{16}\times$信令消息$+CK$，这里 x^{16} 的意思就是将信令消息往高处位移 16 位，然后加上余数。到了接收端，对整个 $T(x)$字段作同样的运算，因为后面已经加了上次未能整除的余数，所以本次一定能整除，如未能整除，说明本次传输过程中有误。

本结论有严格的数学证明，相关的内容请参见本书参考文献 4，本节就不在这里展开。

4. 误差校正

在我们上述过程中如果出现了错误怎么办？校正它！

问题是该怎么校正呢，悟净又想起了当年猴哥教他猴王棒法的经历来。猴哥当年将猴王棒法拆解成九九八十一招，一招招地教他。悟空的棒法从第一招到八十一招都编了序号，称为 FSN 序号。沙僧每学一招也自己标记一个序号，称为 BSN 序号。除了序号，沙僧还有一个标签用来标记自己的学习进度是否跟得上猴哥，这个标签称为 BIB，如果猴哥都教到第 10 招了，但沙僧第 9 招还没学会，沙僧就把第 10 招丢弃不学，同时把 BIB 从“0”转换为“1”给猴哥一个反馈，猴哥自己这里也有一个标签叫 FIB，拿来和 BIB 一比对，这不对啊，我的 FIB 状态还是“0”，这小子的 BIB 状态已经为“1”，两边的进度没有同步哈，沙僧第 10 招都不学直接给我发这个，说明他第 9 招没有学会哈，重教一遍。

图 7.18 所说的就是基本校正法，这显然属于我们之前所说的非互控方式。它是一种既有肯定证实（BSN+1），也有否定证实（BIB 反转）的重发纠错系统。

孙悟空　　沙悟净

FSN　FIB　　BSN　BIB

第6招，亢龙有悔 → 6　0　　5　0　第6招学会了，BSN+1，学会的招数又多了一招

第7招，龙跃于渊 → 7　0　　6　0　如此这般……

第8招，潜龙勿用 → 8　0　　7　0　如此这般……

第9招，飞龙在天 → 9　0　　8　0　太难了，第9招没学会，舍弃，BSN、BIB不变

第10招，龙战于野 → 10　0　　8　0　不是吧，我第9招还不会呢，就来第10招会死人的，得给大师兄一个反馈，我要学第9招BSN不变，BIB反转

…… → 11　0　　8　1

FIB=BIB,从BSN+1重发，BIB反转为1　　继续丢弃的干活

…… → 9　1　　8　1　OK，第二遍终于搞定，下一个

第10招，龙战于野 → 10　1　　9　1

……　　……

图 7.18　悟空教学图

发送端按顺序依次发送信令单元 MSU1，MSU2…。为了便于待会出了错可以重发，它们都被存在发端缓冲器里，直到接收到接收端送来的肯定证实之后，将被证实已正确收到的信令单元从缓冲器中抹去。若收到的是否定证实信令，则说明该 MSU 在发送或传输过程中甚至是接收处理过程中出现了错误。此时，停发新的 MSU，而从由否定证实所指出的那个错误 MSU 开始（即 BSN+1 的信令单元），重发已发出的但未收到肯定证实的信令单元。

重发功能是以下几个参数共同完成的，即前向序号（Forward Sequence Number，FSN），前向指示比特（Forward Indicator Bit，FIB），后向序号（Backward Sequence Number，BSN），后向指示比特（Backward Indicator Bit，BIB）。

FSN 完成信令单元的顺序控制功能，FSN 只给消息信令单元 MSU 分配新的编号，并按顺序发送，在 0～127 循环。而对填充信令单元 FISU 不分配新的编号，只给它前面的 MSU 的 FSN。



BSN 完成肯定证实功能。当收到对方的 FSN 是期望值，即 FSN（对端）=BSN（本端）+1，且该 FSN 序号的 MSU 经误差检测（第 3 部分的内容）是正确的，就将 BSN 加 1，发向对端，否则，BSN 保持不变。

FIB、BIB 完成否定证实功能，并利用值的反转来向对方要求重发。正常情况下，BIB 与另一个方向的 FIB 一致，当一端收到的 MSU 不是期望值时（FSN≠BSN+1），就将 BIB 反转，送向对端，对端收到 BIB，发现与本端的 FIB 不一致，就开始重发，并将 FIB 反转。重发都是从 BSN+1 的消息开始的，如图 7.19 所示。

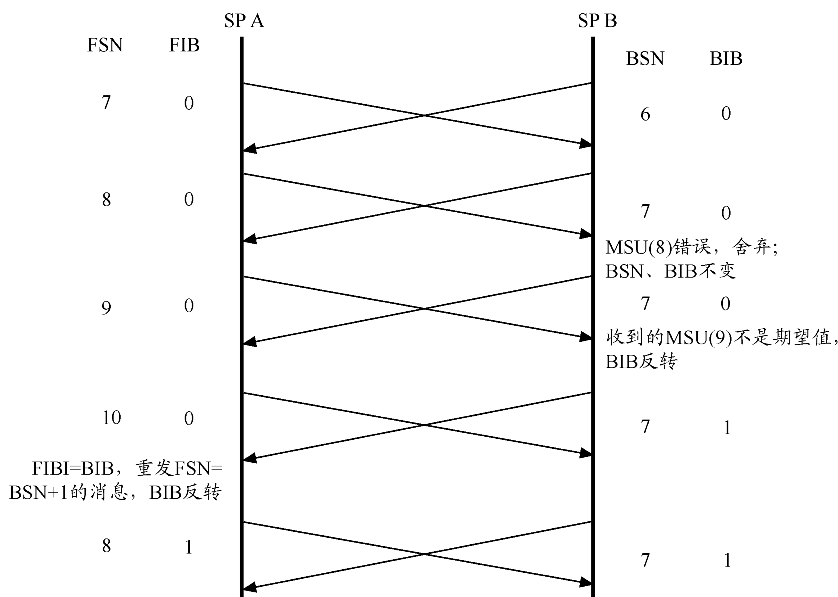


图 7.19　基本校正法

应当说基本校正法不是什么时候都有效的，它适合传输时延小于 15ms 且错误不是太多的链路，对于我们的 2M 电路自然是非常合适的。然而它虽然在不出错的时候效率高，但是出错信息一多就容易造成循环重发，对于传输时延较大的卫星链路，这种循环重发是很要命的。为了解决这一问题，就引进了预防循环重发校正法，主要用于卫星链路。本书的重点是蜂窝通信，不是卫星通信，所以在下面只对这种方法略带提一下。

预防循环重发校正法（PCR 方法）是一非互控、正证实、循环重发、前向纠错的系统，差错校正由发送端主动发送完成。

在这种方法中，发送端发出信令单元后，同时将该信令单元存储在重发缓冲器中，一直到收到该信令单元的正证实为止。在等待正证实信息期间，当无任何新的消息信令单元时，则凡未被证实的消息信令单元自动循环重发。

为防止循环重发队列的过度增长，本方法还规定了强制重发程序，即当未被证实的信令单元数量达到参数值为N_1（$N_1 \leqslant 127$）或未被证实的信令单元的八位位组数量达到参数值N_2时，开始强制重发，即中断发送新的信令单元，而重发存储的准备重发的消息信令单元，直到缓冲器中未被证实的信令单元数及信令单元的八位位组数分别下降至N_1及N_2以下为止。

显然，在传输时延较大的卫星电路中采用这种差错校正方式比采用基本校正方法优越得多。它取消了负证实，不再等待收到了负证实指示后才组织重发，而且凡没有得到证实的消息信令单元一律重发，使对端在重发中接收到正确的消息信令单元。很明显，这种方法对于提高时延大的信令链路的消息传输效率是有效的。使用 PCR 方法校正的差错的示意图如图 7.20 所示。

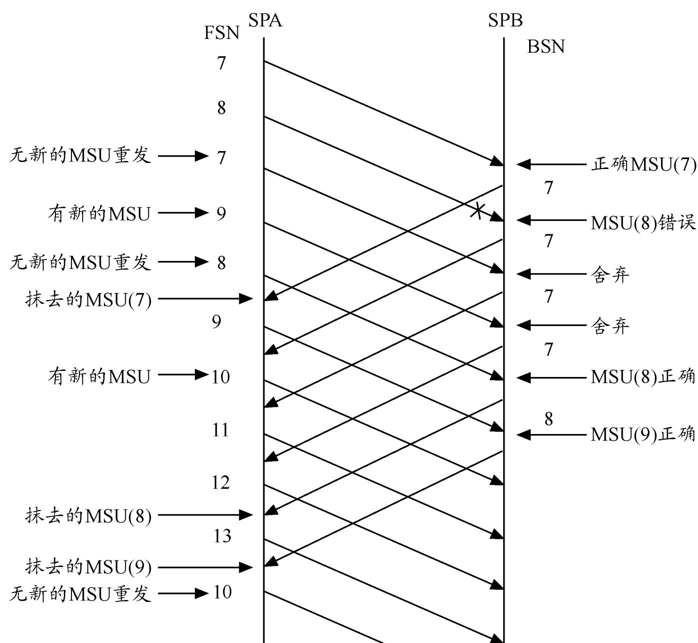


图 7.20　PCR 方法

上面介绍的是两种校正方法，为了在差错检测之后能够对信号进行有效的验证，这需要我们在信令消息原有的基础上增加一些元素，即 FSN、BSN、FIB 和 BIB。这就使得我们的信令单元消息由图 7.15 所示模式变成了如图 7.21 所示模式。

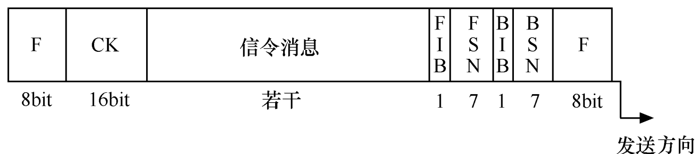


图 7.21　增加了 CK 字段和校正字段的信令单元消息



FSN 和 FIB 各为 7bit 和 1bit 并不令人意外，我们前面说过，FSN 从 0～127 循环计数，也就是有 128 个数字要表示，表示 128 个数字 7bit 当然够了（2^7=128），至于 FIB，一共只有两个表示语，即“0”和“1”，自然 1bit 就足够了。对于 BSN 和 BIB 而言，也是同样的道理。

5. 插入信令单元（FISU）和链路状态信令单元（LSSU）

话说沙僧通过反复钻研差错检测和校正的方法，终于搞定了 ITM 给出的第一笔单子，那就是无差错地传输比特流，不免长舒了一口气。沙僧躺在虎皮沙发上，美滋滋地数着师傅给的第一笔分红，心想这下海来跟随师父创业这一步棋是走对了，咱大小也是个创始人，不再是打工仔了。

没想到几天之后 ITM 又找上门来了，由于沙僧的出色表现。这次他们带来了一份新的合同，要和唐三藏的大唐物流公司建立战略合作伙伴关系，由大唐物流负责给 ITM 公司长期运送比特流。

这次 ITM 又出了三道难题，这几道难题都是针对“长安—虎牢关—洛阳”这条线路目前的安全状况来的。

① 当前土匪横行，妖孽作乱，平时我们不运送比特流的时候，你也应该在路上运点什么东西，好让我们知道这条路没有中断，还能用；

② ITM 公司的企业文化就是“科技以人为本”，人是 ITM 最核心的资源，所以你这条道路上发生了什么意外情况，比如什么“失去定位”、“业务中断”都得及时告诉我们；

③ 新开辟一条道路也好，从妖孽手里把原来已经中断的道路抢回了也罢，先得做验收，验收合格才能投入使用。

这些不消说，都是“把信送给加西亚”的活，都不用去问唐三藏师傅了，沙僧你没得挑，没得跑。沙僧看到这里不由得一阵苦笑，但一想起干完活花花绿绿的钞票，立即又动力十足了。

为了解决第一个问题，沙僧引进了一个叫插入信令单元（Fill-In Signal Unit，FISU）的伙计，这个伙计啥信息不带，啥事不干，通俗一点讲就是一吃闲饭的。当链路上没有 MSU 或者 LSSU 在跑的时候它就冒出来了，为的就是让大家知道这条链路还是好的，没有中断。沙僧对 FISU 的单元格式的初步设计如图 7.22 所示。

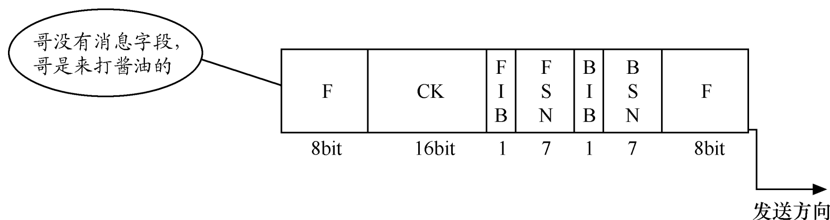


图 7.22　FISU 的设计初稿

第二个问题嘛，也难不倒沙僧，沙僧决定再引进一个叫链路状态信令单元（Link Status Signal Unit，LSSU）的兄弟。这个老兄有个叫 SF 的字段，SF（Status Flag）为状态标志，可以为 8bit 或 16bit，东土大唐的规定是 8bit，目前只用了 3bit，另外 5bit 为备用，其编码如下。

SF：HGFEDCBA

备用 000　　“SIO”　失去定位
001　　“SIN”　正常定位
010　　“SIE”　紧急定位
011　　“SIOS”业务中断
100　　“SIPO”处理机故障
101　　“SIB”　链路拥塞

就这样，悟净设计出来了 LSSU 的初步方案如图 7.23 所示。

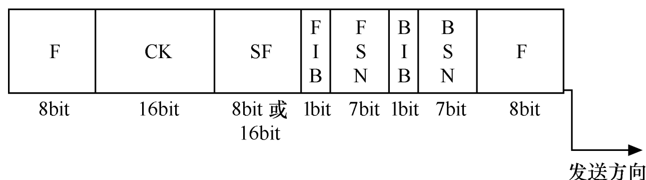


图 7.23　LSSU 的设计初稿

一切看起来都很完美，MSU、FISU、LSSU 都已经就绪，然而问题又来了，如何让处理机很快地辨别这 3 种不同的信令呢？沙僧决定一鼓作气把事情办得漂亮一点，他知道，3 种不同的信令其差别就在于 FIB 与 CK 之间的字段的位数有所不同，于是他在 FIB 字段后面加了一个 LI（Length Indicator）字段，用于标注自 LI 至 CK 中间共有多少 8 位位组，这样就可以让处理机很容易得对 MSU、FISU、LSSU 进行区分。沙僧是这样写 LI 的技术规范的。

LI：长度指示码，指示 LI 至 CK 间的八位位组个数，用于区分 3 种信令单元。当 LI=0，为 FISU，当 LI=1 或 2 时，为 LSSU，而 LI＞2 时，为 MSU。这样就形成了 3 种信令单元格式的最终版本，如图 7.24 所示。

ITM 的第①点要求和第②点要求算是终于完成了，那么第③点要求该怎么做呢，别急，我们且听下面分解。

6. 初始定位

这部分工作是用来应对 ITM 的第③点要求的，一条链路进入业务使用前必须经过初始定位，初始定位是由链路状态信号单元 LSSU 中的 SF 字段来完成的。



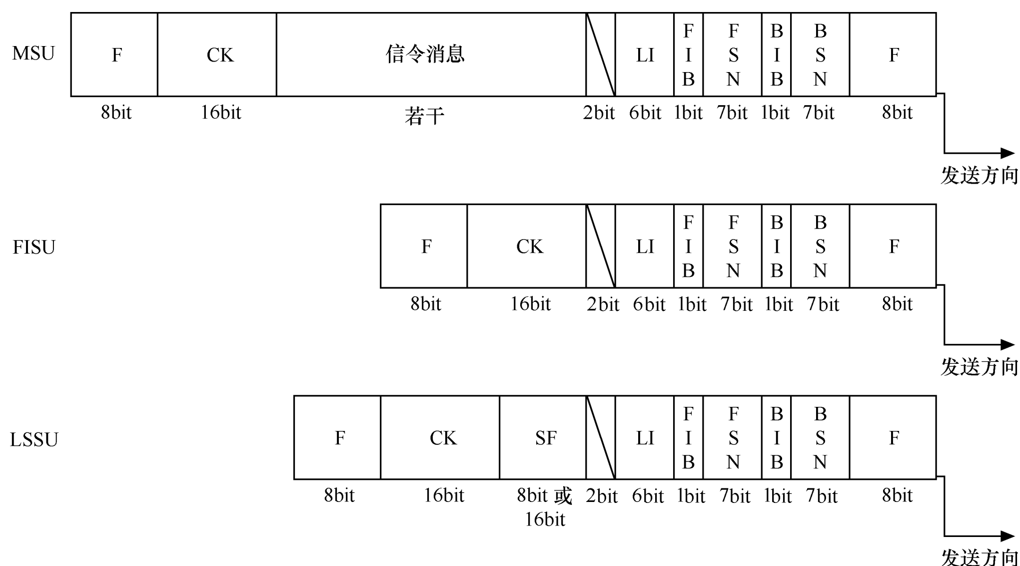


图 7.24　MSU、FISU、LSSU 最终版本

图 7.25 为初始定位的示意图，从图上可以看出。

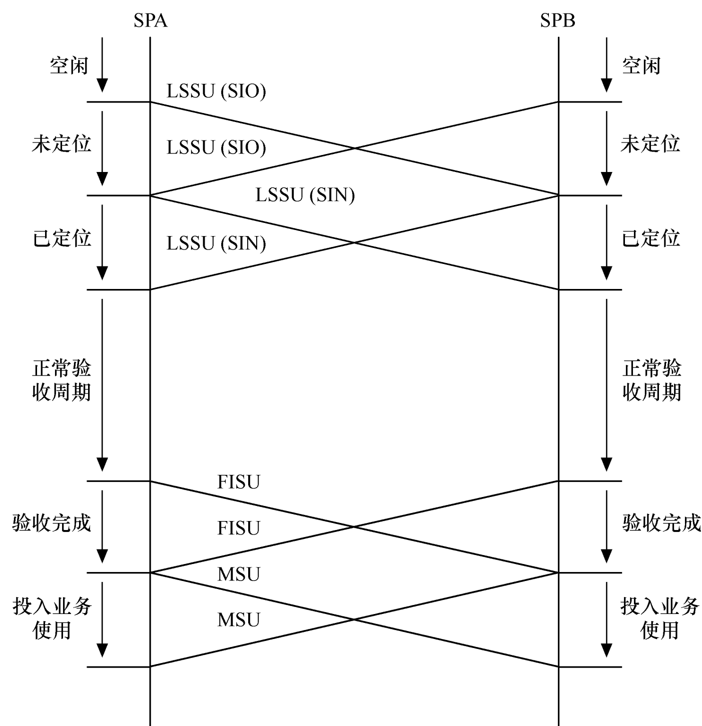


图 7.25　初始定位过程

（1）初始定位过程包括 5 个阶段，未定位—已定位—验收周期—验收完成—投入业务使用。处于空闲状态的信令链决定启动时，信令链两端，即信令点 SPA、SPB 互送 LSSU（SIO），进入未定位状态，并启动定时器 T_2，当双方都收到 LSSU（SIO）时，停 T_2，启动 T_3，互送 LSSU（SIN）进入已定位状态；收到 LSSU（SIN）后，停 T_3，启动 T_4，进入验收周期阶段。

验收是怎么做的呢？在这里要采用一个定位差错率监视程序（见第 7 部分）对信令单元的差错率进行累加，当计数器超过门限 T_i，就认为这次验收合格。若验收合格，且未收到 LSSU（SIOS）或 LSSU（SIO），则完成验收，停 T_4，启动 T_1，进入验收完成阶段；此时双方互送 FISU，以示链路空闲，可以投入业务使用。

对 SIO、SIN、SIOS 不熟悉的朋友请参见本节第 5 点中对 LSSU 信令 SF 字段的描述。

（2）初始定位程序有两种，正常定位（SIN）和紧急定位（SIE）。其区别在于验收周期的时长和计数器的门限不同。正常定位，验收周期为 8.2s，门限 T_i=4；紧急定位，验收周期 0.5s，T_i=1。信令链路使用哪一种定位，由第三层来决定。

（3）在验收周期内，验收须经过 5 次，5 次均不合格才发业务中断 LSSU（SIOS）。

（4）在初始定位过程中，用到 4 个定时器。

T_2：未定位定时器。在初始定位期间发送 LSSU（SIO）允许的最大时延。它应大于传输时延和处理机处理消息所需时延之和，以保证远端能收到 LSSU（SIO）；同时，为保证在故障情况下定位尝试不成功能及早通知第三级进行处理，以便在另一条链路上进行初始定位，T_2 也不能太长。目前我国规定 T_2 的时长为 5～150s。

T_3：已定位定时器。T_3 的时长应不小于传输通路的最大环路时延再加上远端从 SIO 转换到 SIN 或 SIE 所需要的处理时间。我国规定 T_3 为 1～1.5s。

T_4：定位完成定时器。在 T_4 规定时限内，链路必须完成验收投入业务使用，否则，判为故障状态。对于数字信令链路，T_4 规定为 40～50s，建议值为 45s。

T_i：验收周期定时器。对于数字信令链路，正常和紧急验收周期分别为 8.2s 和 0.5s。

7. 数据链路控制级的其他功能

除了对信令消息定界、定位，进行误差检测和校正，对新投入使用的链路进行初始定位以外，还应该在初始定位和链路投入使用之后对差错率进行监视，差错率低的话可以通过重发来校正，但是差错率高的话会引起信令频繁重发，从而产生长的排队时延，所以对信令单元的差错率应该规定一个门限，超过该门限，则判断为链路故障（如图 7.26 所示）。

另外，当由于高于第二级的原因造成链路不能正常使用，就认为发生了处理机故障，处理机故障分为本地处理机故障和远端处理机故障。



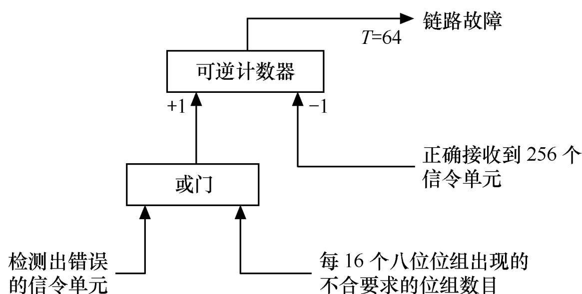


图 7.26　差错率检测机制

当第二级收到了来自第三级来的指示或已判断出第三级故障时，则判断为本地处理机故障。它发送 LSSU（SIPO，处理机故障），并舍弃收到的 MSU。这时，如果对端第二级处于正常工作状态，且仍在发送 MSU 而不是 FISU，则根据收到的本端发送的 LSSU（SIPO），通知第三级连续发送 FISU。

当本地处理机故障消除后，则恢复发送 MSU 和 FISU，只要远端的第二级能正确接收 MSU 和 FISU，就通知第三级恢复正常。

远端处理机故障的处理过程与本地处理机基本类似。

信令链路通过发送 LSSU（SIB）消息进行流量控制。

7.4　八戒掌握了物流调度大权——MTP-3

话说因为沙僧的出色表现，大唐物流公司声名远播，业务也渐渐做大了。西到敦煌，北到雁门，南到巴蜀，都开辟了新路线，唐僧急需优秀的管理人员来辅佐。悟净的执行力无疑是一流的，但在三个徒弟里面，这位卷帘大将的资质显然是最差的，让他做 CEO，唐僧这位董事长还是不放心。斗战胜佛孙悟空毫无疑问地能力出众，问题是他那眼睛里容不得沙子的个性能不能带好一个团队让三藏心里觉得没底，想来想去，想到了八戒，八戒就八戒吧，人家好歹是天蓬元帅出身，管理经验丰富。

主意拿定，唐僧遂从如来身边要回八戒，语重心长地对八戒讲："八戒啊，现在大唐物流做大了，你沙师弟忙着做运输总监，检错纠错，开山劈路，非常辛苦。我这边的事情需要一个人打点，你上任后的主要工作就是要对新铺开的众多业务城市和道路进行管理，物流的调度和管理是大权，汝要慎之又慎，切记切记。"

八戒刚来就被委以重任，自然不敢懈怠。上任第一件事就是给国内各大城市编码，无论是长安、洛阳、成都这样的重镇（SP，Signal Point，信令点）还是虎牢关、潼关、萧关这样的中转站（STP，Signal Transfer Point，信令转接点），都通通编上号。这其实

也是借鉴了大唐邮政的做法，大唐邮政也给大唐境内的城市编了号，发信的时候，邮件的左上角就填收信地址邮编，右下角就写发信地址邮编，一目了然。

八戒也如法炮制，把发信地址称为 OPC（Original Point Code，源点码），收信地址称为 DPC（Destination Point Code，目的地码），当然，从源地址到目的地址可能有多条路径，可能有土路、有高速、有驰道（信令传输中 SP 之间可能有多条路径），这些路用什么标注呢？八戒用 4bit 的链路选择字段 SLS（Signal Link Select）来标注这些不同的道路。这其中 OPC 和 DPC 在大唐境内均为 24bit 编码，SLS 是 4bit 编码，因为七号信令均为八位位组，为了和谐，给 SLS 加了 4 个 0，凑成八位。这就使得信令消息单元又从图 7.21 的格式变成了图 7.27 所示格式。

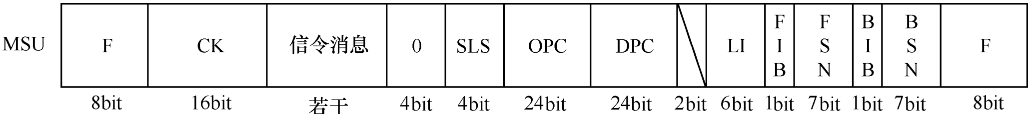


图 7.27　MSU 加上了寻址功能

话说做物流的，自然不是给城市和道路编个号就算完了，对这些道路情况的监控和管理是一项非常重要的工作。哪里的路况出了问题，那么这趟物流可能就要倒到别的路线上去，这称为“倒换 COO”；如果该路线恢复了，就要把物流再倒回来，这称为“倒回 CBD”；有时候几条路况都不怎么好，频繁地倒来倒去，很是烦人，调度部门就不得不出手，强行阻断这条路，先进行维护和测试再说，暂时不让运输大队从这里通行，这被称为“管理阻断 MIM”。

话说这些管理消息实在太多了，八戒想了个办法，把这些消息分为 16 组，用一个 4bit 的 H0 用于识别消息组，每个消息组又分为若干种消息，再用一个 4bit 的 H1 用于识别具体消息。为了方便调度部的同仁记住这些管理消息，八戒画了一张表，如表 7.1 所示。

表 7.1　No.7 信令第三功能级网络管理消息

消息组	H0 \ H1	0000	0001	0010	0011	0100	0101	0110	0111	1000	…	1111
	0000											
CHM	0001		COO	COA			CBD	CBA				
ECM	0010		ECO	ECA								
FCM	0011		RCT	TFC								
TFM	0100		TFP		TFR		TFA					
RSM	0101		RST	RSR								
MIM	0110		LIN	LUN	LIA	LUA	LID	LFU	LLT	（LRT）		
TRM	0111		（TRA）									



续表

消息组	H1 / H0	0000	0001	0010	0011	0100	0101	0110	0111	1000	…	1111
DLM	1000		DLC	CSS	CNS	CNP						
	1001											
UFC	1010		（UPU）									
	1011											
	1100											
	1101											
	1110											
	1111											

表 7.1 中所列消息组如下。

CHM：倒换和倒回消息。

ECM：紧急倒换消息。

FCM：信令业务流量控制消息。

TFM：禁止、允许、受限传递消息。

RSM：信令路由组测试消息。

MIM：管理阻断消息。

TRM：业务再启动允许消息。

DLM：信令数据链路连接消息。

UFC：用户部分流量控制消息。

表 7.1 中常用的命令有倒换 COO、倒换证实 COA、倒回 CBD、倒回证实 CBA、紧急倒换 ECO、紧急倒换证实 ECA、信令路由组拥塞测试 RCT、受控传递 TFC、禁止传递 TFP、受限传递 TFR、允许传递 TFA、禁止目的地信令路由组拥塞测试 RST、业务再启动允许 TRA 等。

（注：关于这些消息的具体用法可谓长篇累牍，由于篇幅和风格的原因本书不打算进行深入解释，请读者自行查阅相关资料。）

除了源地址和目的地地址识别、链路识别和管理消息（如表 7.1 所示）以外，还有传统的八位位组的信令消息，那个才是真正用于网络进行交互的消息。

这几种字符合在一起称为 MSU 的 SIF（Signal Information Field，信令信息字段）。那么 MSU 的结构就变成了如图 7.28 所示。

在将路由的编号与管理等基础工作做扎实之后，八戒开始思考一个 CEO 最重要的工作——业务！准确地说路由的编号与管理应该是技术总监的活，对业务的规划应该是营销副总的工作，然而大唐物流刚刚起步，八戒不得不身兼数职。

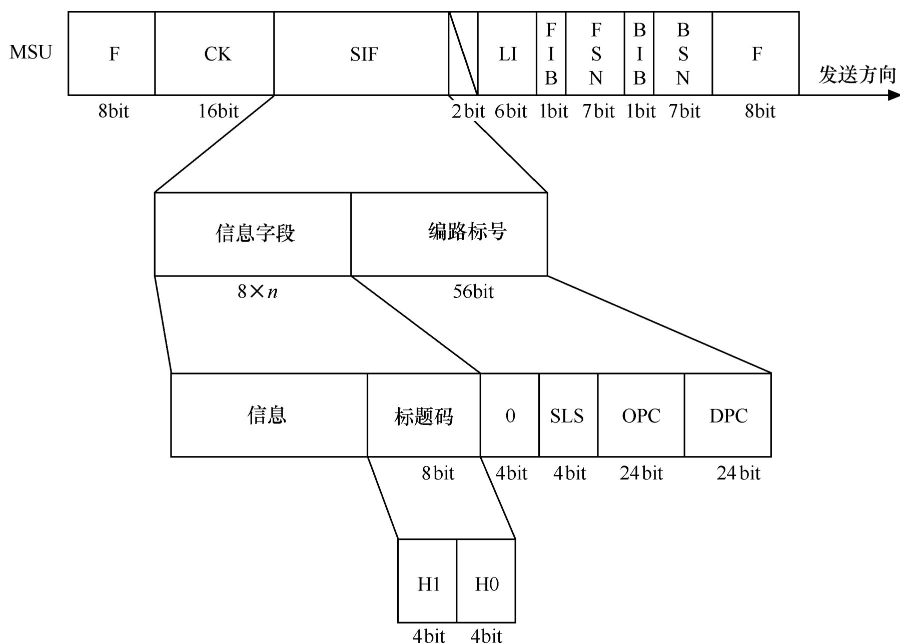


图 7.28　增加了网络管理功能 H0、H1 的 MSU

八戒首先把国际和国内的工作进行区分，他设置了一个 4bit 的 SSF 字段，SSF 字段的 A、B bit 备用，C、D bit 为网络指示语（NI），用于区分国内消息或国际业务消息。国内消息是 14 位或 24 位信令点编码。

比特　　D C B A

0 0 备用　国际网

0 1　　　国内 24 位

1 0　　　国内网

1 1　　　国内 14 位

其次，就是要对物流的各项具体业务进行划分了。很多行业都跟大唐物流做生意，比如家电、家居、建材、粮油、钢铁、化肥、煤炭……八戒在这里设置了一个 4bit 的 SI 字段，用于区分各种不同的业务。

4bit 的 SI 为业务字段，用于指明该 MSU 是到第三级的消息还是到第四级某一模块去的消息。其具体编码如下。

比特　　DCBA

0000　　信令网管理消息

0001　　信令网测试和维护消息

0010　　备用



0011　　SCCP（信令连接控制部分）

0100　　TUP

0101　　ISUP

0110　　DUP（与呼叫和电路有关）

0111　　DUP（性能登记和撤销消息）

其余　　备用

我们刚刚讲到的信令网管理消息（见表 7.1），其 SI=0000。

我们也把 SI 和 SSF 合称为业务信息字段 SIO（Service Information Octet），那么至此一个 MSU 的最终版本终于形成了，如图 7.29 所示。

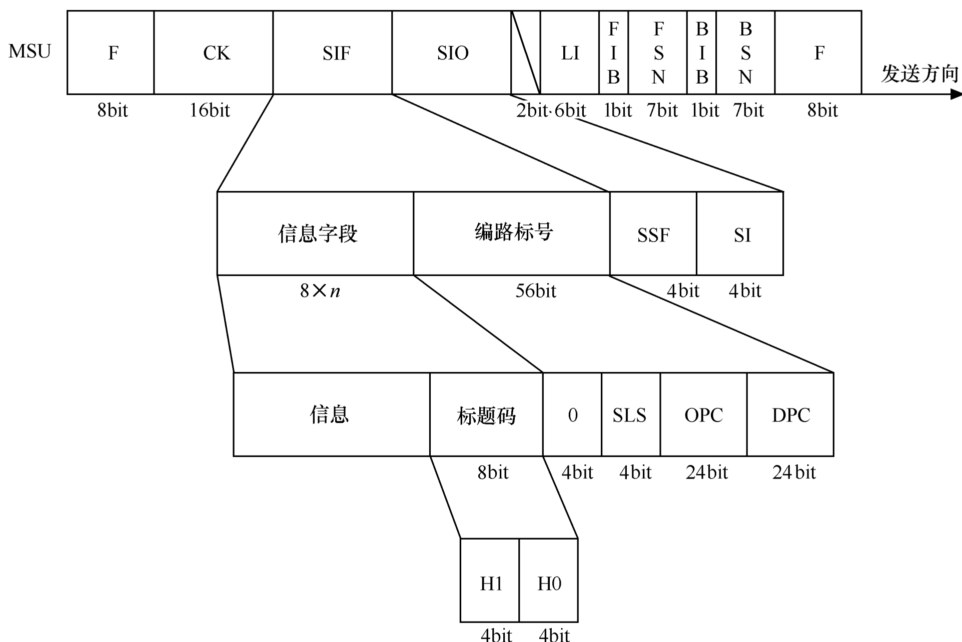


图 7.29　MSU 组成结构（最终版）

话说我们刚刚对从信令点到链路的编号、从管理信息到业务信息讲了一大堆，这些东西该怎么用，下面我们就来进行一下讨论。

信令消息处理功能是用来保证源点的用户部分产生的信令消息传递到该用户指明的目的地的相同用户。

（1）消息编路功能

如果源信令点 OPC 要把信息发送出去，或者是信令转接点 STP 要把信息进行转发，显然首先要做的工作就是路由的选择。

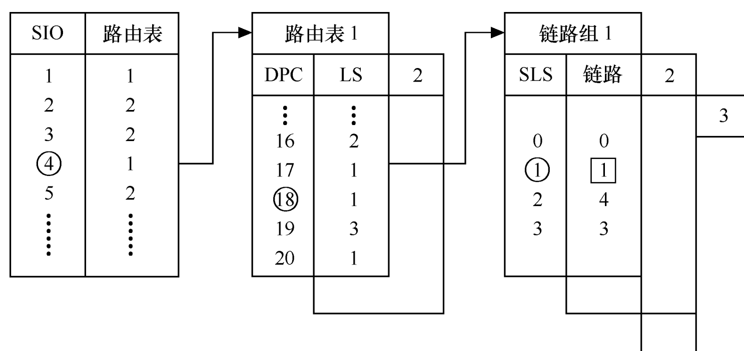
我们可以根据 SI、DPC、SLS 来选择到达某一目的地的路由中的一条信令链。具体步骤如下。

当第 3 层消息或第 4 层消息需要发送时，那么路由的选择就是一个必不可少的过程。七号信令由 MTP-3 中的消息路由功能为待发的消息选择消息路由。如果两信令点间有两条或多条信令链路可将信令业务传递到同一目的地点，要采用负荷分担的方法，将这一信令业务在这些链路之间分配。

消息路由的选择是以预先确定的路由数据为基础，通过分析路由标记中的目的地编码（即 DPC）和信令链路选择码（SLS）来完成的。在某些情况下，还需利用业务信息八位位组中的 SI 和 SF 来完成。

消息路由功能确定到达目的地路由中的一条信令链路要有 3 个步骤。第 1 步是根据业务信令八位位组字段 SIO 中的 SI 选择信令业务使用的路由表，这是由于不同的业务（比如 TUP、ISUP）可采用不同的信令路由。但如果信令网中不同的业务都使用同一路由表的话，这一步可以省略；第 2 步是根据所要达到的目的地，即 DPC 来选择使用的信令链路组；第 3 步是根据 SLS（或 SLC）在信令链路组内选择一条信令链路。

消息发送时，消息路由的选择过程可由图 7.30 来说明。



图中，SIO：业务信息8位位组；DPC：目的地编码；
LS：链路组；　　　　SLS：信号链路选择

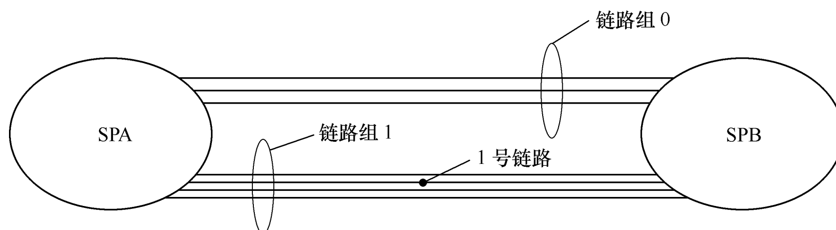


图 7.30　消息发送时消息路由选择示意图



由图 7.30 可以看出，SIO＝4、DPC＝18、SLS＝1 的信令消息将经过 1 号信令链路组中的 1 号信令链路传送。

消息路由功能在选择发送消息的信令链路时所涉及的信令路由表、信令链路组、信令链路数据，是在交换局开局时设计并生成的。在局数据中除了这些数据外，还有信令路由、链路组信令链路的优先级及当前状态的数据等，这些数据也将在消息路由选择中使用。这些路由信息可以通过人机命令进行补充和修改。

（2）消息鉴别功能

首先根据目的地 DPC 可判定该消息的终点是不是本信令点。若不是则本信令点为转接点，继续将信令发给其他信令点。

（3）消息分配功能

当一个消息到达某一信令点时，首先执行消息鉴别功能，将收到的 DPC 与接收点本身的编码进行比较，若不一致，则不是本信令点，须经过本信令点执行消息编路功能进行转接。若一致，则是到本信令点的，接着执行消息分配功能。

消息分配功能把信令消息分配给本信令点的相应用户部分。由于信令点的 MTP 部分可能要为多个用户服务，因此决定信令消息分配给哪一个用户部分，主要依靠分析信令消息中的业务信息八位位组 SIO 中的业务指示码（SI）来实现。

当 SI 字段等于 0000 或 0001 时（即待分配的消息为信令网管理消息或信令网维护和测试消息），还要分析标题码 H0、H1 的编码，以确定将消息交由哪个信令网管理功能部分处理。

7.5 孙悟空重出江湖——SCCP

有句俗话说的好，这世界上没有无缘无故的爱，也没有无缘无故的恨。这话用到 SCCP 和 MTP 身上也同样适用。MTP 的三层结构无疑取得了很大的成功，它和 TUP（Telephone User Part，电话用户部分）一起完美地完成了大多数的通信。随着业务的发展，MTP 慢慢显现出它的弱点来，比如不适合传递与电路无关的消息，DPC 寻址的能力有限，SI 字段能支持的业务种类有限，不能建立面向连接的虚电路从而发送大量非实时消息等。现代通信的迅速发展，让 MTP 的不足显得愈发突出，SCCP（Signal Connect Control Part，信令连接控制部分）由此应运而生。

话说三藏的大唐物流公司有两位徒弟的鼎力相助，每天要做的事情就是躺在沙发上点钞票和斜倚在卧榻上睡觉。睡觉睡到自然醒，数钱数到手抽筋，呃，这可比在西天天



天打坐念佛舒服多了。

不过八戒的短板也随着公司的高速发展很快显现出来，首先是八戒人比较懒，只肯和大公司做大业务（呼叫业务，与电路相关），不肯去做一些快递之类的小业务（GSM中的漫游通信、位置更新、呼叫转移等业务，与呼叫电路无关），而这些业务对物流公司的发展相当重要；其次，八戒是用 DPC 和 OPC 来对国内的物流点（信令点）进行编号，然而大唐是按 24bit 进行编码的，国际是按 14bit 进行编码的，无法实现国际物流，这让唐僧觉得相当不满，因为从和白龙马创建公司时起他就想把公司打造成一个全球一流的物流公司；再次，八戒是用业务信息字段 SIO 中的 SI 来定义具体的业务种类，SI 总共只有 4bit，4bit 只能支持 16 门类，可是大唐的业务早不止什么建材、汽车、钢铁、煤炭等传统业务的物流了，随着社会的发展好多物流业务像雨后春笋一般涌了出来，比如行李托运、网络购物、鲜花礼仪、月饼寄送等，4bit 根本无法支持大唐物流公司日益扩大的业务种类需求；最后，八戒还被一些国际巨头，如报捷、联合华丽、普辉联合投诉了，说他搞的 MTP-3 层不肯为这些巨头开辟专门的物流通道（建立虚电路）用以方便地传送大量的物资（虚电路通过预先建立连接的方式用于传递大量的非实时信息），这些巨头还威胁，internet 公司能提供虚电路业务，你们 telecom 公司要是敢不提供虚电路，我们就要集体改投 internet 的门下了。

唐僧面对这成堆的问题和无休无止的投诉，一个头都两个大了。想来想去他想到了悟空，唐僧总是这德性，平时总是信赖八戒和悟净，走投无路的时候才想起大徒弟悟空。也罢，大唐物流就要上市了，八戒的能力无以担任上市公司的总裁，那就让他当副总裁，CEO 还是让悟空来做，多给八戒一些股份作为补偿就是了。

话说悟空在西天也非常无聊，他是个好动的人，佛门又是一个清静之地，每天打坐念经的，很不对他胃口。偶尔有些打打杀杀、降妖除魔的活又都让金刚罗汉们包揽了，根本轮不到他这个佛出手，这个斗战胜佛沦为了一个打坐念经佛，着实让他很不爽。所以唐三藏一召唤，说给他个上市公司的 CEO 当当，悟空大喜过望，立马就向如来辞行，一个筋斗云直奔东土大唐而去。

话说悟空到了东土，立马组织了一个部门叫做 SCCP 部（Signal Connect Control Part，信令连接控制部分），该部门职权在八戒的 MTP-3 之上，统管公司业务。该部门首要的任务就是要解决八戒的一些遗留问题。

话说八戒从 CEO 位置上退了下来，虽然当了副总裁又多分了股份，心里还是多少有些不爽。但对于大师兄，他从来都是敢怒不敢言，但是总还是喜欢小小反抗一下以示他这个天蓬元帅的存在。

SCCP 部门刚筹建就有属下满脸委屈地向悟空告状——MTP 层有八戒撑腰根本不听指挥，理都不理他们，就算是那些业务部门比如 MAP、BSSAP、ISUP、INAP 也一个个



摆架子，不把他们当回事。悟空一听大怒，立即下发了第一道总裁函：“即日起，位于 SCCP 层之上的应用层和位于 SCCP 之下的 MTP 层，都给我设置一个或多个叫 SAP 的接口（Service Access Point，业务接入点），层与层之间通过接口进行信息交互。为了避免口说无凭和互相推诿，层与层之间的工作交流必须采用工单，工单也称原语。MTP 层与 SCCP 层的通信，采用‘MTP-’原语；应用层和 SCCP 层的通信，采用‘N-’原语，各部门敢违抗总裁令的，金箍棒伺候！”

悟空金箍棒的厉害人尽皆知，此令一下，各部门莫不噤若寒蝉，只得照章奉行。该工单由 4 部分组成，其格式如下。

层标识	属名	专用名	参数

①“层标识”表示提供业务的功能块，如：MTP-表示是 MTP 和 SCCP 间的原语，N-表示是 SCCP 和其用户间的原语；

②“属名”说明该功能块应提供的服务，如：UNITDATA 表示传递单元数据，NOTICE 用于进行通知，CONNECT 用于建立连接，DISCONNECT 用于拆除连接。属名的作用就是让对方知道该干什么，相当于工单的标题。

其中，SCCP 用户（不妨理解为业务部门吧）给 SCCP 层打的工单称为 N-原语，都有如下类型，如表 7.2 所示。

表 7.2　　　　用于网络服务的 SCCP 用户原语

原　语　名	原语类型	协议类别				原语参数
		0	1	2	3	
N-UNITDATA 单元数据原语	请求	√	√			CDA CGA SEQ RO UD
	指示	√	√			CDA CGA UD
N-NOTICE	指示	√	√			CDA CGA RR UD
N-CONNECT 建立连接原语	请求			√	√	CDA CGA RCS EDS CI
	指示			√	√	QOS UD CI
	响应			√	√	RA RCS EDS CI
	证实			√	√	QOS UD CI
N-DISCONNECT 拆除连接原语	请求			√	√	RA REA UD CI
	指示			√	√	OR RA REA UD CI
N-DATA 数据原语	请求			√	√	CR UD CI
	指示			√	√	

续表

原　语　名	原 语 类 型	协 议 类 别				原 语 参 数
		0	1	2	3	
N-EXPEDITED DATA 加速数据原语	请求				√	UD CI
	指示				√	UD CI
N-RESET 复位原语	请求				√	REA CI
	指示				√	OR REA CI
	响应				√	CI
	证实				√	CI
N-INFORM 报告原语	请求			√	√	REA QOS CI
	指示			√	√	

表示原语参数缩写的含义为：

CDA：被叫地址　CGA：主叫地址　CI：连接识别号　CR：证实请求
EDS：加速数据选择　QOS：服务质量参数集　OR：发信者　RA：响应地址
RCS：接收证实选择　REA：理由　RO：回送选择　RR：回送理由
SEQ：顺序控制　UD：用户数据

SCCP 部门给 MTP 打的工单也称为 MTP-原语，如表 7.3 所示。

表 7.3　MTP-业务原语

原　语		参　数
原语名	特定名	
MTP-TRANSFER	请求	SCCP 消息
	指示	
MTP-RESUME	指示	受影响信令点
MTP-PAUSE	指示	受影响信令点
MTP-STATUS	指示	受影响信令点
MTP-UPU	指示	受影响信令点

其中，部分 MTP-业务原语含义如下。

MTP-TRANSFER 请求：SCCP 用于接入 MTP 的信令消息处理功能。

MTP-TRANSFER 指示：MTP 的消息处理功能把信令消息传送到 SCCP。

MTP-PAUSE 指示：由 MTP 发送，表明它不能把消息传送到指定的目的地。



MTP-RESUME 指示：由 MTP 发送，通知用户 MTP 有能力提供到指定目的地的 MTP 业务。

③“专用名”指示了原语的类型，通俗一点讲就是发工单呢还是收工单，亦或是工单反馈。OSI 定义了 4 种原语，如图 7.31 所示，其分类功能如下。

- 请求原语（Request）：高层用户向下层请求一种功能，比如说 SCCP 部门给 MTP 部门发工单要求办一件事。
- 指示原语（Indication）：服务提供者向高层请求一种功能或通知高层一种功能已在 SAP 里完成。
- 响应原语（Response）：用户通知下层已完成原先在 SAP 点由指示原语请求的功能。
- 证实原语（Confirm）：服务提供者通知高层已完成原先在 SAP 点由请求原语请求的功能。

这 4 种原语的顺序是：请求→指示→响应→证实。

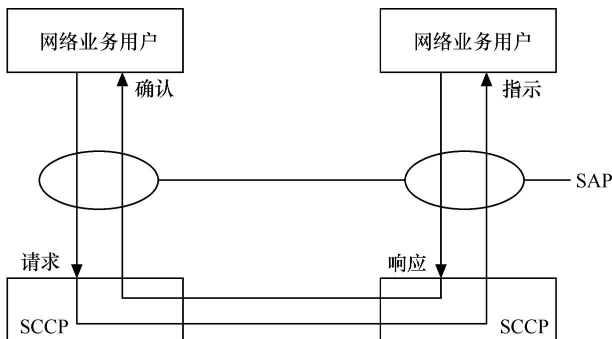


图 7.31　原语类型

④“参数”为层间要发送的信息，可以理解为“②‘属名’”的扩充说明。比如说“属名”为 N-NOTICE 的通知原语就有 CDA（被叫地址）、CGA（原叫地址）、RR（返回原因）、UD（用户数据）4 个可选参数。

我们看到，N-原语和 MTP-原语加起来一共有 18 种。

整肃了部门的风气以及规范了工作流程之后，悟空这位强势的 CEO 开始着手考虑解决那些影响业务发展的问题。

首先是一些国际大公司提出的面向连接的物流通道问题。在这个问题上，悟空借鉴了另一家物流公司 internet 公司的做法，将业务划分为无连接业务和面向连接业务。internet 公司是通过 UDP 和 TCP 两种协议来实现的，但悟空并不想那么麻烦，他就打算用 SCCP 来实现这两种功能。

1. 业务

悟空将 SCCP 的业务按照是否面向连接划为四类：0 类和 1 类是无连接型，2 类和 3 类是面向连接型，即 0 类是基本无连接业务，1 类是有序无连接业务，2 类是基本的面向连接业务，3 类是流量控制面向连接业务。

（1）无连接业务

无连接业务实质上是分组交换中的数据报业务，不需要事先建立连接就可以传递信令，数据报的传递是通过逐段转发来实现的。

它把应传送的数据信息利用单元数据消息（UDT）——这种消息在 GSM 里面使用得很普遍——从发端 SCCP 节点作为独立的消息直接发送出去。图 7.32 为无连接业务示意图，图中各个 SCCP 节点之间传送着互不相关的 UDT（可能来自不同的用户）。中继 SCCP 通常指两个不同信令网的连接点，用来连接两段 SCCP 链路。如果发生故障使中继 SCCP 不能传递该 UDT 时，就向发端返送 UDTS 消息用于说明无法传递的理由。

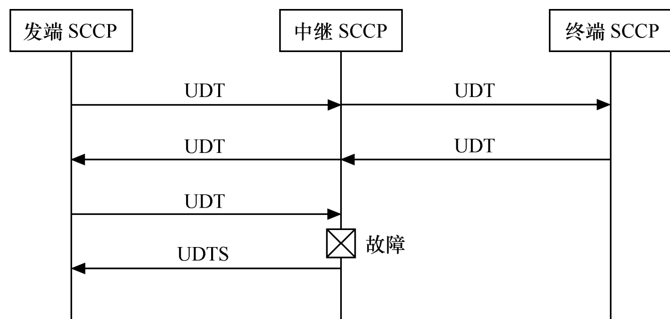


图 7.32　无连接业务

在 0 类业务中，各个消息被独立地传送，相互间没有关系，所以不能保证按照发送的顺序把消息送到目的地信令点。在 1 类业务中，给来自同一信息流的数据信息附上了同一信令链路选择字段 SLS，就可保证这些数据信息经由同一信令链路传送。因此，可按发送顺序把消息送到目的地信令点。无连接业务每发一次数据，都需重选一次路由。

（2）面向连接业务

面向连接业务实质上是分组交换中的虚电路方式，即在传送数据之前，需要先建立逻辑连接；传送数据之后，要拆除逻辑连接，如图 7.33 所示。在 2 类业务中，由于各个数据消息不带顺序号，因此不能完成顺序控制和流量控制。在 3 类业务中则可以完成顺



序控制和流量控制。

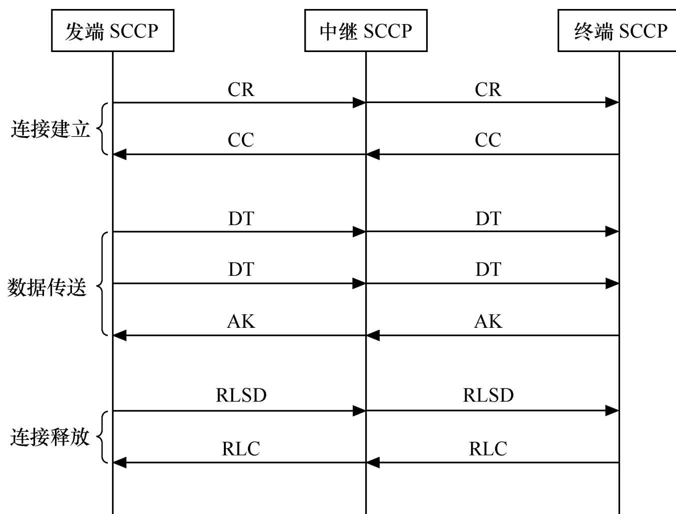


图 7.33　面向连接业务

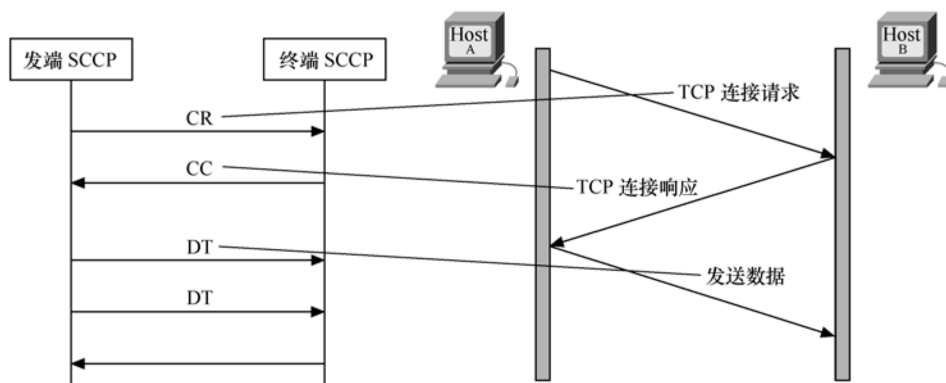


图 7.34　SCCP 与 TCP 的对比

请注意，图 7.33 比图 7.32 多了一个连接建立与释放的过程，连接建立的过程与 TCP 连接建立的过程也很相似，我们来看看 TCP 的经典的“三次握手”建立连接的方式，如图 7.34 所示。

面向连接业务又分为暂时信令连接和永久信令连接。暂时信令连接是指信令连接的建立和拆除需要由 SCCP 用户启动和控制，类似于拨号电话接续；永久信令连接是本地（或远端）的 O&M（操作维护中心）功能，或者由节点的管理功能建立和释放，用户无法控制，他们为 SCCP 用户提供半永久连接，类似租用电话线路。

面向连接业务适用于传送数据量大，实时性要求不高的业务；而无连接业务适用于数量不大，有实时性要求的业务。

目前，智能网业务 INAP，移动电话业务 MAP 和 ISUP 基本都采用无连接 SCCP，当需大量的网管数据信息时可采用面向连接的 SCCP。

2. 消息格式

悟空定义了部门之间的沟通语言——工单（即原语）之后，解决了部门之间政令不通的问题。然后以雷霆手段，将 SCCP 部门的业务支持划为两种，即支持实时性强的无连接业务和实时性不需要很强但是需要传递大量数据的面向连接业务，这使建立虚电路成为可能，从而缓解了国际巨头的投诉危机。

现在他开始把眼光投向内部，他需要整肃内部的工作流程，以使整个公司的工作都规范化。这个内部工作流程的整顿就是通过岗位说明书的方式规定每一个位置的岗位（每一个消息块），所占的资源多少（比特数），以及要完成的工作，这个就是 SCCP 的消息格式。

SCCP 消息同信令网管理消息、TUP 消息一样，是采用信令单元的方式在信令链路上传递，它们的区别在于 SIO 中的业务字段 SCCP 不同。当 SI=0011 时，信令单元传递的消息为 SCCP 消息（如图 7.35 所示）。

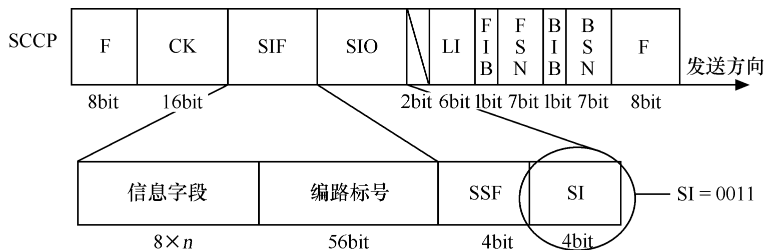


图 7.35　SCCP 消息

图 7.36 是 SCCP 消息的 SIF 的具体内容，它是由整数个 8 位位组组成的。发送时先发送顶部 8 位位组，后发送底部的 8 位位组，而在每个 8 位位组中，从最低有效位开始发送。

（1）编路标号

大家对比一下图 7.36 和图 7.37 可以看出，MTP 消息和 SCCP 消息在路由标记上并没有什么不同，都是由目的地码（DPC）、源点码（OPC）、链路选择字段（SLS）3 部分组成，SCCP 把与 MTP 不同的寻址功能放到了参数里面。



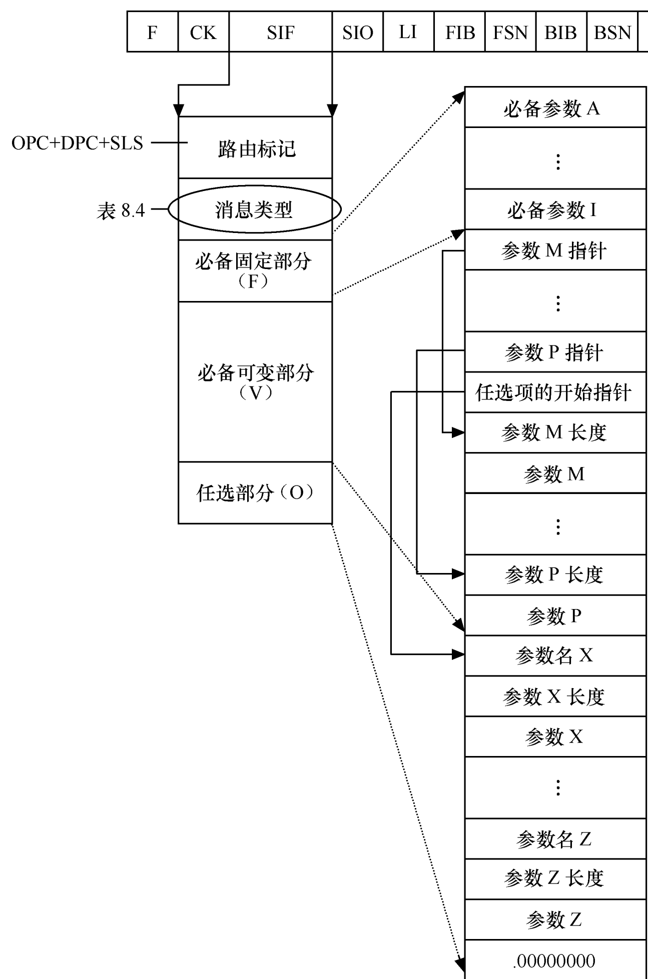


图 7.36　SCCP 消息格式

（2）消息类型编码

为了完成 SCCP 功能，共规定了 18 种用于网络服务的消息，如表 7.4 所示。对这些消息每种分配一个消息类型编码，来区分不同的消息，它对所有的消息都是必备的。

表 7.4　SCCP 的消息类型及编码

功能分类	消 息 类 型	协 议 类 别				编　码
		0	1	2	3	
连接建立	CR 连接请求			×	×	00000001
	CC 连接确认			×	×	00000010
	CREF 拒绝连接			×	×	00000011

续表

功能分类	消 息 类 型	协 议 类 别				编　　码
		0	1	2	3	
连接释放	RLSD 释放连接			×	×	00000100
	RLC 释放完成			×	×	00000101
数据	DT1 数据形式 1			×		00000110
	DT1 数据形式 2				×	00000111
	AK 数据证实				×	00001000
	UDT 单位数据	×	×			00001001
	UDTS 单位数据业务	×	×			00001010
	ED 加速数据				×	00001011
	EA 加速数据证实				×	00001100
初始化	RSR 复原请求				×	00001101
	RSC 复原确认				×	00001110
其他	ERR 协议数据单元错误			×	×	00001111
数据	增强的单元数据（XUDT）	×	×			00010001
	增强的单元数据业务（XUDTS）	×	×			00010010

×：此消息可在对应的协议类别中使用。

（3）参数部分

① 必备固定部分

对于一个如上（2）所述的消息类型，有些参数是必不可少且长度固定的。这部分参数放在必备固定部分。消息类型规定了这类参数的位置、长度和顺序，所以在参数中不需要包括该参数的名字和长度指示码。

② 必备可变部分

对于一个如上（2）所述的消息类型，有些参数是必不可少但是长度是可变的。这部分参数放在必备可变部分。

每个参数开始由指示字表明，这个指示字不妨理解为编程里的指针，它指出了从指示字开始到参数之间有多少个 8 位位组，其实也就是个寻址功能。比如指示字“00000001”指明相关的参数在指示字之后的第一个 8 位位组开始，中间没有别的信息。当然，如果不止一个参数，那就不会有“00000001”指示字了，指针后面连的还是指针。

必备可变部分的开始部分是逐一排列所有的指示字，然后根据指示字去寻址具



体的参数。每个具体的参数开始的一个 8 位位组总是参数长度指示码，后面接参数的内容。

在长度可变的参数部分，最重要的就是地址信息参数了。我们之前介绍八戒的 MTP–3 部门的短板时，有一条就讲的是 MTP-3 的寻址能力太差。这个问题在 SCCP 里是怎么解决的呢？

下面让我们回顾一下 MTP 的寻址功能（如图 7.37 所示）。

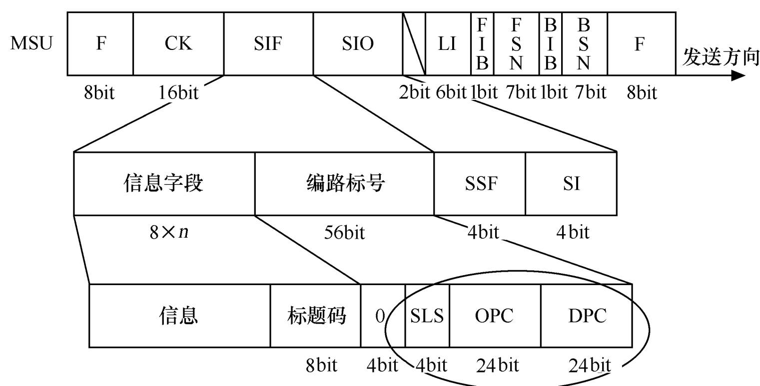


图 7.37　MTP 的寻址功能

我们看到了 MTP 就是采用 OPC、DPC、SLS 来寻址，这种做法有一个显而易见的缺点，那就是当两个不同的设备采用同一个 DPC 进行编号时，你打算怎么办，如何区分它们？这种情况还真存在，比如说 HLR/AuC 就是集成在一起的，MSC/VLR 也是如此。如果把 DPC 比喻成门牌号码，那这就好比同一个门牌号码的大楼里驻扎了两个机构一样，光靠门牌号码是没法区分了，你得想别的办法。

悟空设计了一个 SSN（Sub-System Number，子系统号）来解决同一门牌对应几个不同机构的问题。

SSN 用于识别 SCCP 的用户，由一个 8 位位组组成，其编码如表 7.5 所示。

表 7.5　SSN 编码

比 特 序 号	**HGFEDCBA**
00000000	未定义的子系统号/没有使用
00000001	SCCP 管理
00000010	备用
00000011	ISDN 用户部分
00000110	操作维护管理部分（OMAP）

续表

比 特 序 号	HGFEDCBA
00000101	移动应用部分（MAP）
00000110	归属位置寄存器（HLR）
00000111	拜访位置寄存器（VLR）
00001000	移动交换中心（MSC）
00001001	设备识别中心（EIR）
00001010	鉴权中心（AuC）
00001100	智能网应用部分（INAP）
11111111	扩充备用
其他	备用

SSN 的启用不仅解决了如何识别子系统的问题，而且相比 MTP 的 SI 字段，这里多了 4bit（SI 只有 4bit），这就大大扩大了大唐物流的业务经营范围。对于 DPC 的弱点，不能进行国际漫游寻址没有什么帮助，于是，就有了 GT（Global Title）码。目前交换设备是采用 E.214 方式进行编码，也称为“MSCID”。结构形式如下：

E.214=E.164+E.212

例如：86130H0H1H2H3××××。前面采用 E.164 的 CC 和 NDC，后面采用 E.212 的 MSIN，这是因为 E.164 格式比较适合在网络中传输。

应当说具体的 GT 码格式远比我们刚才所说的要复杂，它还要包括全局码的翻译类型、编号计划和编码方案。由于篇幅和整体风格的限制，我们在这里不一一介绍，请大家自行查阅相关的书籍。

在 SCCP 的构架中，DPC、SSN 和 GT 构成了完整的 SCCP 主被叫地址。SCCP 的主被叫地址是一个 SCCP 消息的一部分，准确地说是参数，我们会通过任务的分解来一步步还原 SCCP 消息。

主叫/被叫用户地址是长度可变的参数，用来准确地识别源点、目的地点及 SCCP 接入点。在无连接业务中，它表示消息传送的起点和终点，类似于 MTP 编号标号的 DPC 和 OPC；在面向连接业务中，它只用在连接建立过程中，表示信令连接的起点和终点，与消息传递的方向无关，一旦连接建立好了，就好比修了一条高速公路，我从高速的起点走到终点就好了，不需要知道起点和终点的具体地址。主叫/被叫用户地址参数结构如图 7.38 所示。



图 7.38　主叫/被叫用户地址参数结构



地址指示码用于指示包含在地址字段中地址信息的类型，比如是否包括信令点码、是否包括子系统号以及是从 GT 还是 DPC+SSN 选取路由等信息，在这里不再详加讨论。

③ 任选部分

除了必不可少的部分之外（必备固定部分以及必备可变部分），SCCP 消息还有任选部分，任选部分和必备部分一样，也分为固定长度和长度可变两种。每一任选参数应包括参数名、长度指示码和参数内容。如果有任选参数，则在任选参数发送后，发送全 0 的 8 位位组表示“任选参数结束”。

我们说了这么久的参数，下面就来看看 SCCP 消息类型的参数都有哪些（如表 7.6 所示）。

表 7.6　SCCP 消息的参数

参　数　名	编　　码
任选参数结束	00000000
目的地本地参考	00000001
源本地参考	00000010
被叫用户地址	00000011
主叫用户地址	00000100
协议类别	00000101
分段/重装	00000110
接收序号 P®	00000111
排序/分段	00001000
信用量（credit）	00001001
释放原因	00001010
返回原因	00001011
复原原因	00001100
误差原因	00001101
拒绝原因	00001110
数据	00001111
分段	00010000
跳计数器	00010001



3. SCCP 消息及用户最终数据的生成

我们知道，对于互联网也好，七号信令网也罢，用户数据信息都是自顶层一级级向下封装而得来的。这些信息都是怎么封装的呢，我们来举一个例子，如图 7.39 所示。

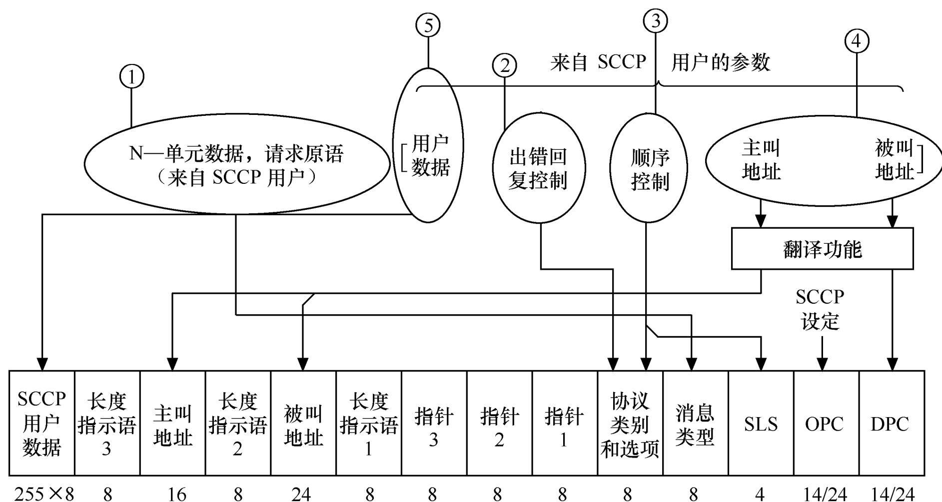


图 7.39　用 N-原语形成 SCCP 消息（UDT）

① 根据原语名和原语类型生成“消息类型”参数，原语为 N-UNITDATA 消息，那么根据原语就生成一个 UDT 单元数据消息。

② 根据原语参数中的回送选择参数（RO）确定是否要求后续节点 SCCP 在无法传送本消息时将原消息送回，据此确定“协议类别”参数的 5～8bit。

③ 根据原语参数中的顺序控制参数（SC），确定协议类型。如果要求消息有序发送，则视为 1 类协议，否则为 0 类协议。据此确定“协议类别”参数的 1～4bit。若为 1 类协议，则根据 SC 参数值确定 SLS 值，否则随机选择一个 SLS 值。

④ 根据原语参数中的主叫地址参数（CGA）和被叫地址参数（CDA），经过 SCRC 功能模块的翻译和处理，转换成 UDT 消息中的主叫地址和被叫地址，并得到 MTP 寻址的 DPC，同时填入本节点的 OPC 码。

⑤ 将原语参数中的用户数据原封不动地装入 UDT 消息的“用户数据”字段。

上面的部分我们讨论的是对于一个“N-原语”，如何将其翻译成 SCCP 消息，接下来我们要做的是将 SCCP 消息翻译成 MTP 消息。我们首先把 SIO 字段中的业务指示语 SI 置为 0011（SI=0011），指示 MTP 其用户为 SCCP，接下来对 SCCP 消息进行封装。

这样就形成了“N-原语”→“SCCP 消息”→“MTP3 消息”→“MTP2 消息”的逐层封装，如图 7.40 所示。



图 7.40　用户消息的逐层封装

应当说八戒（MTP-3）和悟空（SCCP）这前后两位大唐物流的 CEO 在公司的战略层面上并没有本质的区别，有了沙师弟（MTP-2）在下面任劳任怨地完成点到点的无差错物流工作。处于高层的八戒（MTP-3）和悟空（SCCP）绝大多数时候只需要考虑如何很好地完成物流的调度。应当说八戒的“OPC+DPC+SLS”的管理模式已基本足以应付绝大多数寻址了，但随着国际业务的发展和子系统的诞生（比如 MSC 和 VLR 的合设），这种方式就不足以应付现代通信的需求了，于是就诞生了悟空的“GT+SSN”，SSN 相当

于 SIO 字段中的 SI 的扩展，SI 原来只有 4bit，SSN 有 8bit，一下子可以支持的业务或者可识别的子系统就由 16 个到了 256 个，这算是悟空体系对八戒体系的扩展。

在“MTP-3”体系中，所有的数据都是加上源地点和目的地点发出去的，跟 internet 上的 UDP 消息一样，事先不需要建立连接，也没有固定的路径依赖。对于实时性比较强的数据和并非数据量很大的数据，这样做是很有必要的，因为事先建立连接，开辟一条虚电路是需要浪费时间和资源的，这种情况下电路交换（虚电路）远没有分组交换来得有效率，可是对于大量的和实时性不是那么强的数据，那么建立虚电路进行有序和大量的传送显然是有必要的。在这方面，SCCP 更像是 TCP 和 UDP 的结合，既可以提供无连接业务又可以提供面向连接业务，有效弥补了 MTP-3 不能进行面向连接的传送的不足。

原语并非 SCCP 所独创，原语是用于层与层之间交流的，我们在本节中介绍了 MTP-原语和 N-原语，下节中我们还要介绍 TACP-原语。原语的属名说明要触发的动作，专用名用于说明消息的走向，参数你不妨理解为对属名要触发的动作的阐述。应当说这几个名词很生涩，并不好理解，我们用一个武术动作来对其进行解读。比如“白鹤亮翅——收回左拳护腰，乘势将左足向前踢一寸腿，同时右手再向前发一冲拳……”，那么这里的属名就叫做“白鹤亮翅”，说明将要做的动作；专用名就是“进攻对手”，白鹤亮翅是一手攻招，四个专用名“请求—指示—响应—证实”说明了原语的流向，你不妨理解为“进攻对手—对手挨打—对手反攻—本人挨打”；参数就是对“白鹤亮翅”的具体阐述，“左拳护腰”、“左足前踢”、“右拳向前”就是具体的参数。SCCP 层具体消息的参数已在表 7.6 中列出。

SCCP 层要承接 N-原语和向 MTP 层发 MTP-原语，算是原语最丰富的地方，所以七号信令的教材讲原语都从 SCCP 层开刀，本书也不例外。消息的层层封装都是原语所触发的，在图 7.39 和图 7.40 中我们对这个问题加以了阐述。

MTP 层还有一个问题就是它以前都是 TUP 触发的，属于呼叫触发型，对于固网而言，这基本就够了。但是对于移动网而言，因为用户位置的不断变化，就算不打电话时也要进行信令的交互，比如说你漫游到了新的 MSC 下面，VLR 需要从 HLR 里调取你的数据存到本地，这与话路没有关系，你打不打电话这个过程都是必需的，位置更新和鉴权与此也类似。MTP 算是老革命遇到了新问题，然而 SCCP 就没有这个麻烦，它可以由 TCAP 触发。TCAP 是一个统一的接口，MAP、INAP、OMAP 都经过它加工后可以由 SCCP 进行处理。在移动网中，与话路无关的信令实在是非常多，这也是 SCCP 诞生的重要理由。

本节开始的时候我们就说过，没有无缘无故的爱，也没有无缘无故的恨。现在我们要说的就是：“SCCP 也不是无缘无故从天上蹦出来的，它就是历史的必然，它就是群众的呼声，它就是为移动通信革命而生的！”



7.6　长袖善舞的太白金星——TCAP

我们在上一节中已经说过了，无论是 SCCP 层也好，MTP 层也罢，关注的都是网络层的问题，即如何完成信令消息的调度（寻址），如何提供无连接和面向连接的信息交互。然而需要进行通信的实体又是如此之多，比如 OMAP、MAP、INAP 等，而且这个阵容还在不断扩大，处理各种不同的消息是很复杂的。按 OSI 的理念，层与层之间的工作应该有清晰的区分，SCCP 既然关注的是网络层的东西，它就不应该再去关注和懂得具体的业务，专业才能铸就品质。SCCP 需要应对的是一种固定的格式，这种固定的格式就好比一个筐，MAP、INAP 或者新增的一些应用服务通通可以往这个筐里扔，SCCP 只需要考虑如何把这个筐进行打包进行传送，而并不需要考虑筐里装的到底是什么，这个筐的工作就由本节要提到的 TCAP 来完成，这也是本章开始就提到的泰勒的科学管理的理念。

就好比你去肯德基喝饮料，服务生应该先给你个杯子（TCAP），你可以随便在这个杯子里装什么饮料，可乐（OMAP）、雪碧（INAP）、芬达（MAP），然后把杯子（TCAP）放在盘子（SCCP）上，用盘子把这些东西运走。盘子是不会去考虑杯子里到底装的是什么饮料。

或许有人并不同意，反对意见就是 SCCP 层和 MTP 层也要考虑封装的对象的，论据就是 SSN 指示语和 SI 指示语。如果把邮局打包裹的大麻袋比作 SCCP 或者 MTP 的话，那么 SSN 和 SI 就相当于一个标签，往这个麻袋上“啪”地一贴，表明麻袋里装的是土豆还是地瓜，便于你解开麻袋的时候辨认，但无论装的是土豆也好，是地瓜也罢，麻袋的封装方式是不会为此而改变的。

话说大唐物流的业务越做越大了，OMAP、MAP、INAP 通通冒了出来，为了应对这些业务，唐僧在各地建立了一些叫 HLR、VLR 的大仓库，OMAP、MAP、INAP 就可以直接去仓库里取。但是问题也很快就出来了，一是业务太多了，格式各不相同，这使得 SCCP 的封装有点困难，SCCP 部门希望专门有人可以出面和 OMAP 等打交道，以免 OMAP 等再去纠缠专门搞调度的技术人员；二是各色人等都可以去仓库取东西，仓库管理员的眼睛都看花了，另外 OMAP、MAP、INAP 这帮人交货习惯和行为方式还各不相同，搞得仓库管理员无所适从啊，于是仓库管理员强烈要求建立一个物资管理部，所有业务都只跟物资管理部打交道，然后物资管理部来仓库提货，这样就符合 ISO9000 质量认证标准了，也就规范化了。

唐僧觉得这些建议都言之有理，为了节省开支，他并不想多增加部门，于是就跟悟



空商量，想让悟空在 SCCP 增设一个处理业务的中心。没想到悟空一口拒绝了，悟空的理由是专业人做专业事，他那里的都是专业技术人员，去搞业务没道理，业务和调度也不适合放一个部门，还拿出 OSI 的文件精神给唐僧看——诺，OSI 是讲究分层的。唐僧没辙，就打算筹建一个市场部，专门管理这些业务。想来想去，他还是觉得天上地下，就数太白金星交游最广，佛家道家通吃，西天天庭人脉都不错，于是决定邀请太白金星来担任市场部部门经理兼副总裁，主管营销。

太白金星是何许人也，那是三清之一，道教的领袖啊，如果跟猴子八戒搞得一样，那岂不很失水准。于是他决定要玩酷的，虽说内容并不复杂，但是名字一定要搞得很酷，让你们都看不懂。哼，如果你们都能看懂我在玩什么，俺还能叫太白金星吗。他首先把自己的部门命名为 TCAP（Transaction Capabilities Application Part，事物处理能力应用部分），然后规定了和这些业务单元的工单叫做“TC-原语”，和 SCCP 的工单称为“N-原语”，这不过是抄袭了孙猴子的杰作，没啥创意。结果背后就有人指指点点，说这太白金星贵为三清，也是天地神仙的领袖之一，抄袭一个猴子的东东，实在有伤大雅。

太白金星闻之大怒，你们都看得懂是吧，看懂了显不出我三清的水平来了是吧。那好，俺就跟你们玩点玄的，玩玄的对俺来说还真是小儿科，你们看王重阳、张三丰、王阳明那些道家的后辈，哪个不会玩玄的，何况太白金星我！太白金星这一怒不要紧，他创造的 TCAP 的新名词可是坑苦了学通信的后辈们，人人学七号信令只要一听到 TCAP 就摇头啊，那些词汇太莫名其妙了。

太白金星将 TCAP 分成了两个子层，分别称为成分子层 CSL（Component Sub-Layer）和事物处理子层 TSL（Transaction Sub-Layer），两个子层之间用“TR-原语”进行通信。而成分子层 CSL 又分为对话处理和成分处理两部分。TCAP 层的结构如图 7.41 所示。

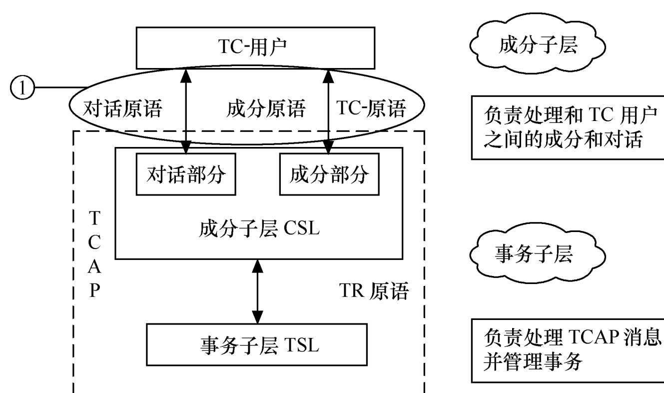


图 7.41　TCAP 的分层结构



成分、对话、事务，我相信大多数人都要晕了。之所以晕不是因为这些词汇我们不熟悉，而是因为太熟悉了，然而又完全不是我们日常生活中的意思，所以在大脑里两个概念会打架。你非要把英语重新编写过，说“tree”是猫的意思，“dog”是跑步的意思，我相信学过一点英语的人大脑也会被搅成一团浆糊，这就是太白金星的厉害之处，人家就是喜欢玩玄的，就是让你搞不懂！

我们还是从上往下看过来，第①部分讲的是原语，原语我们并不陌生，它就是用来实现层与层之间通信的，我们的各种消息就是通过原语自上而下生成的。然而，一般情况下层与层之间只用一种原语，但是 TCAP 的用户和 TCAP 之间居然有两种原语，叫做成分原语和对话原语，这实在让人觉得很晕，七号信令本来就够复杂了，你搞两种原语这不是添乱吗？

要解释这两种原语的区别我们还是绕不开那几个词汇：“对话”、“成分”和“事务”。

什么叫成分呢？一个操作是由远端要执行的一个动作，它可以带有相关的参数。一次操作请求或响应。我相信这种解释是没有办法让大家对“操作”和“成分”这两个词产生联想的。成分来源于单词“component”，是组成成分的意思。那么所谓的“成分”是谁的组成成分呢？那就是对话。

那什么是对话呢？为了完成一个应用，两个 TC 之间所有的操作以及操作返回的信息就构成了一个对话，简单地说，一个业务过程就是一次对话，一个对话通常是包含多个成分的。所以成分就是对话的“component”。

什么叫做事务呢？事务就是网络两节点间处理的业务，事务与对话之间有一一对应的关系。

我们举一个例子来说明这 3 个概念。你去银行给老乡汇款，那么给老乡汇款这件事本身就是一项“事务”。为了完成这项“事务”，你需要先填汇款申请单，然后请营业员帮你转账，转账时营业员会给你一张确认单，你填完确认单之后这笔业务才正式宣告结束。填汇款申请单也好，填确认单也罢，这都被称之为“成分”，那么完成这一系列的操作就被称作一个“对话”。

TCAP 这样做的好处在于它的通用性，而与具体的应用无关。它是将信息传递功能与呼叫控制功能分开，传递与电路无关消息的统一的协议。为了支持其通用性，TCAP 将消息交互过程看作“事务”或者“对话”，其中包括一次或多次“操作”，每次操作由本端调用，由远端执行，并回送操作执行结果。这样的一次操作请求或响应，就构成 TCAP 消息中的一个成分，若干成分按一定顺序组合成 TCAP 消息中的事务处理部分。这种统一的消息结构和语法规则适用于所有的 TC-用户，每个成分的信息含义及成分顺序包含用户信息，与具体应用有关，取决于 TC-用户。

如图 7.41 所示，TC-用户与 CSL 成分子层之间采用 TC-原语接口，TC-原语又分

为成分处理原语和对话处理原语；CSL 成分子层与 TSL 事务子层之间采用采用 N-原语接口。

（1）TC-原语之成分处理原语

如同我们前面所说的，成分处理原语就是用来处理操作和应答的，共有 9 种，它是一个完整的“对话”的组成部分。下面列出了原语的名称、类型和功能（如图 7.42 所示）。

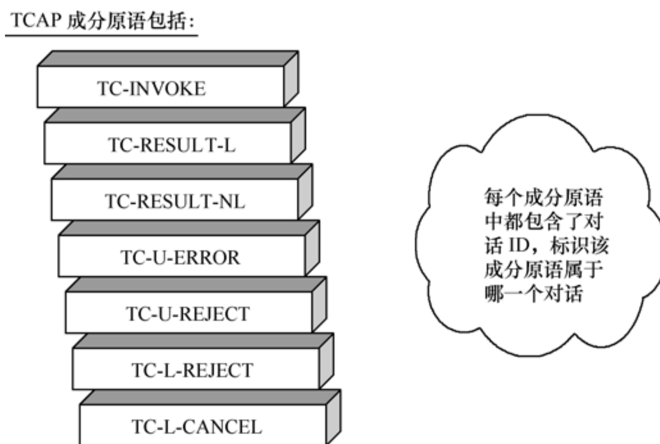


图 7.42　TC 成分原语

TC-INVOKE 调用（请求，指示）：一个操作的调用。

TC-RESULT-L（请求，指示）：成功执行的操作结果。

TC-RESULT-NL（请求，指示）：成功执行的操作分段结果的非最终部分，说明结果还没完，还在继续。

TC-U-ERROR（请求，指示）：对一个以前调用的操作的回答，指明操作执行失败。

TC-L-CANCEL（指示）：通知本地 TC-用户，一个操作调用因时限到而终止。

TC-U-CANCEL（请求）：TC-用户将撤销决定通知本地成分子层，都是撤销，一个是由时限引起的，另一个是由用户引起的。

TC-L-REJECT（指示）（本地拒绝）：成分子层通知本地 TC-用户，收到的成分无效。

TC-R-REJECT（指示）（本地拒绝）：成分子层通知本地 TC-用户，收到的成分被远端成分子层拒绝。

TC-U-REJECT（请求，指示）：TC-用户拒绝由其同层实体产生的它认为不正确的成分。都是拒绝，前两者是因为成分子层引起的，最后这个是因为 TC-用户引起的。

（2）对话处理原语

对话处理原语用来请求或指示与消息传递或对话处理有关的子层功能。当事务处理



子层用来支持对话时，这些原语对应到 TR-原语（如图 7.43 所示）。

TC-UNI（请求，指示）：请求/指示一个非结构化对话，我们一般不用。

TC-BEGIN（请求，指示）：开始一个对话。

TC-CONTINUE（请求，指示）：继续一个对话。

TC-EN（请求，指示）：结束一个对话。

TC-U-ABORT（请求，指示）：表示用户层放弃，用户层告诉 SP 信令点，由于用户原因操作对话被放弃。

TC-P-ABORT（指示）：由于对话的格式不被 TCAP 所理解，被 TCAP 层放弃。

TC-NOTICE（指示）：当 TCAP 要进行一次对话，结果传送到 SCCP 层时由于网络原因导致不能传送，SCCP 层会通知 TCAP 由于 SCCP 层本身有问题，让 TCAP 转告用户，TCAP 则通过 TC-NOTICE 告诉它的用户。

（3）TR-原语

TR-原语与 TC 原语中的对话处理原语有一一对应的关系，即 TR-原语也有 7 种，分别为：TR-UNI、TR-BEGIN、TR-CONTINUE、TR-END、TR-U-ABROT、TR-P-ABROT、TR-NOTICE，如图 7.44 所示。

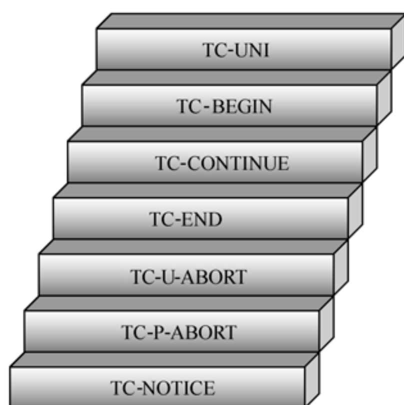


图 7.43　TC-对话处理原语

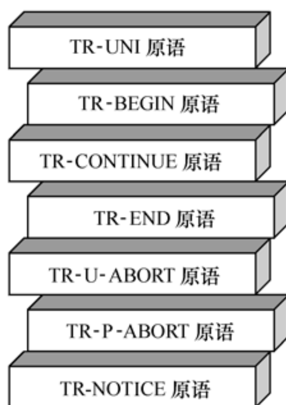


图 7.44　TR-原语

虽然我们在上面对“成分”、“对话”和“事务”进行了解释，也对所包含的原语种类进行了解析，但相信还是没有打消多数人的疑虑。那就是同样是为了进行操作，为什么要分为“对话”和“成分”两个部分？既然“对话”和“事务”有一一对应关系，那么设置两个子层有何必要呢？

对此，我们举一个例子来进行解释。这个 TCAP 的各种行为就好比拍电视剧，演员的或哭或闹、一笑一颦都是在导演的掌控下完成的，导演的指令和演员的动作都可以称为“成分”。比如说导演用 TC-INVOKE 原语调用演员开始哭，演员就用 TC-RESULT-L

向导演展示一个梨花带雨的哭的场面。有些演员比较大牌，导演的每一个指令不一定都执行，比如说李小龙，有一次导演让他演一个场景，也就是用拳打一个泰拳演员，结果泰拳演员纹丝不动的场面，就被李小龙返回了一个 TC-L-REJECT 指令，对不起，我的截拳道如此之牛，对方是不可能站着不动的，我一拳就要让他趴下！这些“成分”都要有一个 ID，这就相当于每个动作都归属于某集电视剧一样，你拍的时候就应该给这些动作一个编号，好归口管理到一集电视连续剧里去（一个对话）。

问题是这电视剧不是说拍就拍的，导演、演员、灯光、摄影都得准备好才能开始，所以我们看到拍片的时候，导演都会拿一块牌子，口中开始倒计时“Action——开拍！”，这 TCAP 也是如此，它用 TC-BEGIN 开始一个对话，用 TC-CONTINUE 继续一个对话，用 TC-END 结束一个对话。任何操作要进行，都必须先启动对话，“对话”是对“成分”的管理，没有对话是无所谓成分的。就好比导演还没说开始拍戏，演员在那里瞎“操作”（瞎“成分”）都是没有用的，是编不进电视剧的。

“成分”和“对话”分开颇有点承载和控制分离的意思，“成分”承载了操作动作，“对话”是对“成分”的控制。“成分”的传送用 TC-原语中的成分处理原语完成，但是否要发送成分或者接收成分，需要用 TC-原语中的对话处理原语来控制和通知。

话说这“对话”和“事务”的关系就更让人费解了，明明是一一对应的，搞两个东东是不是有点劳民伤财，这两者到底有什么区别？

我们首先来比较一下 TC-BEGIN 原语和 TR-BEGIN 原语的不同，这两者之间虽然是一一对应的，但是具体内容就有很大的不同。TC-BEGIN 原语只是 TC 用户通知 TCAP 准备启动一次对话，并不包含成分；但是 TR-BEGIN 原语是由成分子层（CSL）送给事务处理子层（TSL）的，它既包含启动对话的信息，也包含相关的成分。与此类似，TR 这些成分都既有对话信息也有成分信息。

其次，“对话”更偏重于微观层面的管理，“事务”更侧重于宏观层面的管理。这是什么意思呢，比如说 2008 年的奥运会开幕式，就有总导演和节目导演之分，“对话”相当于一个节目导演，它要做的就是完美地完成自己的那个节目；而“事务”就相当于总导演了，每个“对话”都在它那里有备案，它要负责管理这些“对话”，并把所有的节目进行封装（变成 TCAP 消息），提供给观众（SCCP）。

我们应当注意的是，TR-原语并不是 TCAP 层工作的尽头，它还需要把这些信息进行封装打包提供给 SCCP 层，再由 SCCP 层封装给 MTP 层。

我们下面来看一个具体的例子，通过例子来讨论一下 TCAP 的信令过程到底是如何实现的？

（1）成分子层处理过程

成分子层处理过程包含对话处理和成分处理。



图 7.45 为一次成功的成分处理过程。首先由信令点 SPA 的 TC-用户发起一次操作，向本端的成分子层（CSL）发送调用请求原语 TC-INVOKE，该 CSL 利用收到的 TC-INVOKE 形成调用成分，并动态分配 INVOKE ID（标识一个操作）为 I。远端节点 B 的 CSL 接收该调用成分，并用 TC-INVOKE 的指示原语送给 TC-用户。节点 B 的 TC 用户将操作结果分别用最终结果 TC-RESULT-L 请求原语、返回结果（最终）成分（INVOKE ID 也等于 I，标识是同一个操作）和 TC-RESULT-L 指示原语反方向送到信令点 SPA 的 TC 用户，如图 7.45 所示。

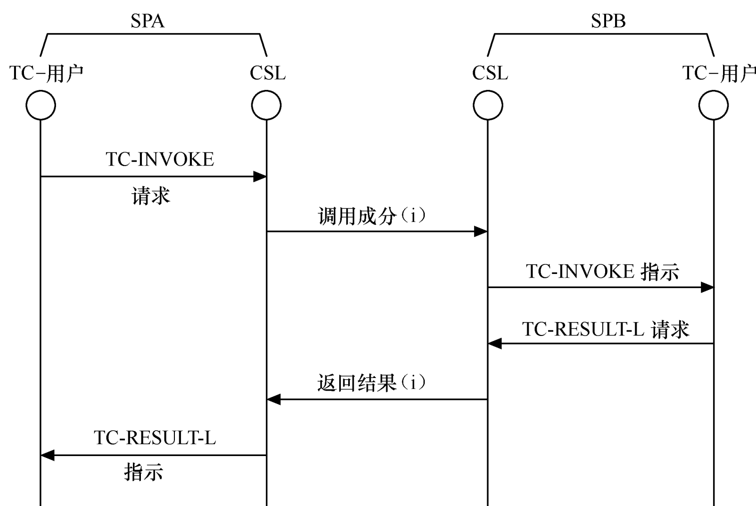


图 7.45　正常的成分处理过程

这里有几点要注意。

① INVOKE ID 由发端成分子层分配，一个 TC 用户不需要等待前一个操作完成，就可以调用另一个操作。也就是说允许任何时刻，可以同时有多个并发的操作在远端执行。不同的操作用 INVOKE ID 来区分，属于同一操作的调用或结果成分，含有相同的 INVOKE ID。

② 当收端收到一个操作并执行时，需发端继续提供信息，于是向发端发出一个操作请求，这个操作有自己的 INVOKE ID，同时还带有前面收到的 ID，此处称为链接 ID，表明为了执行前面的操作才请求调用这个操作。

③ 成分子层通常还通过对话 ID 将成分与一个特定的对话相联系。

（2）事务处理子层过程

图 7.46 所示为一次正常的事务处理子层过程。首先 SPA 的 TR 用户（即 CSL 层）用 TR-BEGIN 请求原语启动一次事务处理，TSL 将原语进行处理封装形成 BEGIN 消息（TCAP 消息），其中 OTID（Original transaction ID，起源事务处理 ID，用于标注一个事

务）等于 X，送到 SPB。收到 BEGIN 消息后，TR-BEGIN 的指示原语送到 SPB 的 TR 用户。若 SPB 的 TR 用户决定建立事务处理，就将 TR-CONTINUE 请求原语送到 TSL，并形成 Continue 消息传送到 SPA，Continue 消息含有 OTID 和 DTID（Destination transaction ID，目的地事务处理 ID），其中 OTID 等于 Y，DTID 等于 X，因为源地址和目的地址反过来了。然后有 TR-CONTINUE 指示原语送到 TR 用户。若想结束事务处理，有两种方法，一种称为基本方法，即任何一端的 TR 用户通过 TR-END 原语和 END 消息终结事务处理；另一种称为预先安排的方法，即预先安排在应用的某一给定点释放事务处理，这时，只发送 TR-END 请求原语，不发送 END 消息。

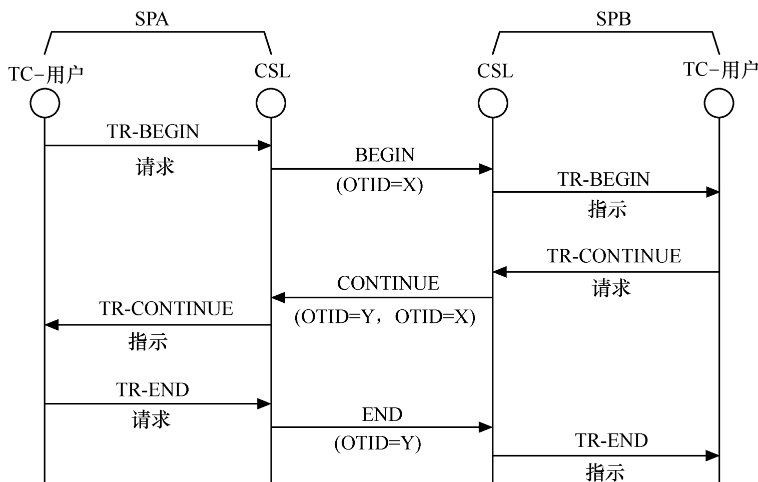


图 7.46　事务处理子层示例

这里应注意以下两点。

① 事务处理 ID 用来识别事务处理，每个节点在启动事务时，分配它本身的本地事务处理 ID，在事务处理过程中保持不变。

② TCAP 消息中的成分部分在事务处理子层原语中作为用户数据，在成分子层和事务处理子层之间通过。

我们之前提到了 MTP 层、SCCP 层和 TCAP 层，设计这些层次的目的都是为了承载在其之上的应用层。对应 GSM 而言，最重要的就是 MAP 消息和 BSSAP 消息。这两部分消息与信令流程联系非常紧密，我们就不在这里加以详述，而将其放到第 8 章里面。

图 7.47 算是本章内容的总览，图中最下面的内容是 MAP、BSSAP，也就是应用部分，打包放入 TC 层的成分部分。TC 层的消息又打包装入 SCCP 层的数据部分。SCCP 层的消息又封装到 MTP-3 的信息内容部分。



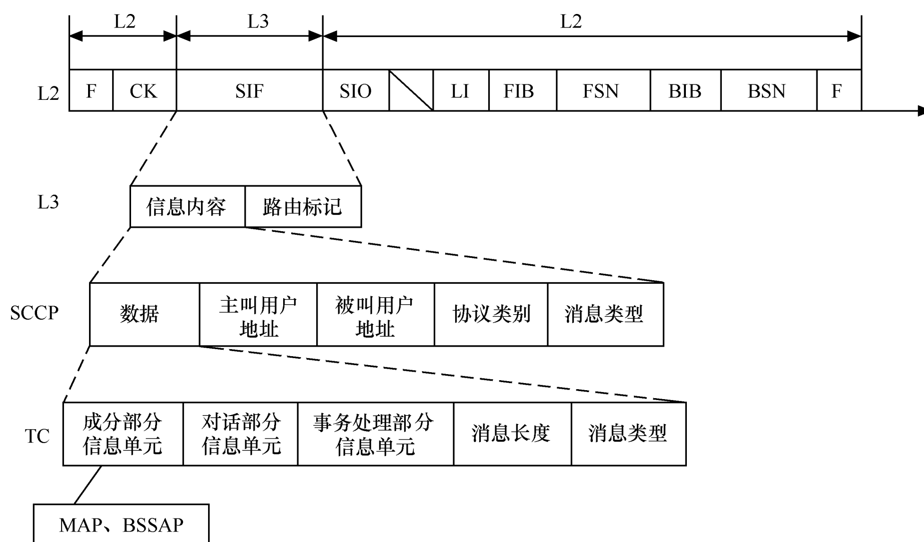
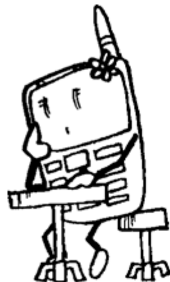


图 7.47　从应用层到 L2 的一层层封装

由此我们也可以看到，七号信令的封装方式与 TCP/IP 没有本质的区别，都是自上而下层层封装。

第 8 章

Chapter 8



妙手著文章——通过信令流程让 GSM 系统运作起来

GSM 协议是一种语言，一种 GSM 设备之间进行沟通的语言，这与人类社会也颇有相似之处，人类社会也要通过语言进行沟通，从而共同完成某项事情。如果把第 6 章的第三层协议和第 7 章的七号信令理解为一门语言的单词和语法的话，那么第 8 章要做的事情就是把这些单词和语法串联起来形成一篇文章，一篇让 GSM 体系为之运作的文章，也称之为“信令流程”。信令流程在 GSM 网络的维护和优化中具有非常重要的地位，只有对 GSM 的信令流程有清楚的认识和理解，才能对网络进行深入的分析。不仅如此，学习信令流程还对了解一个真正的商业蜂窝系统的运作机制大有裨益，无论是 GSM 还是 CDMA，亦或 WCDMA，在信令流程上都有颇多相同和相似之处。

如果把“第 4 章商业蜂窝通信系统的典范——GSM”理解为 GSM 的骨架的话，那么第 8 章就是 GSM 网络的灵魂和精髓之所在。一如大唐的三省六部制，所谓的中书、门下、尚书 3 省和吏部、户部、礼部、兵部、刑部、工部 6 部只是一个王朝的骨架。要研究透一个王朝，隐藏在骨架之后的律法、税赋制度、科举制度、田亩制度才是其要义。

应当注意的是，第 6 章的第三层协议和第 7 章的七号信令并没有涵盖 GSM 网络中的所有信令，我们在第 8 章开始的时候需要对 GSM 网络的接口和信令再进行一番整体的探讨。

8.1 GSM的信令与协议

8.1.1 接口与协议

接口与协议是有所不同的，接口代表两个相邻实体之间的连接点，而协议是说明连

接点上交换信息时需要遵守的规则。协议是各功能实体之间的语言，两个实体要通过接口传递特定的信息流，这种信息流必须按照规定的语言传递，双方才能相互了解，这种语言就是协议。图 8.1 所示为 GSM 网络的各个接口。

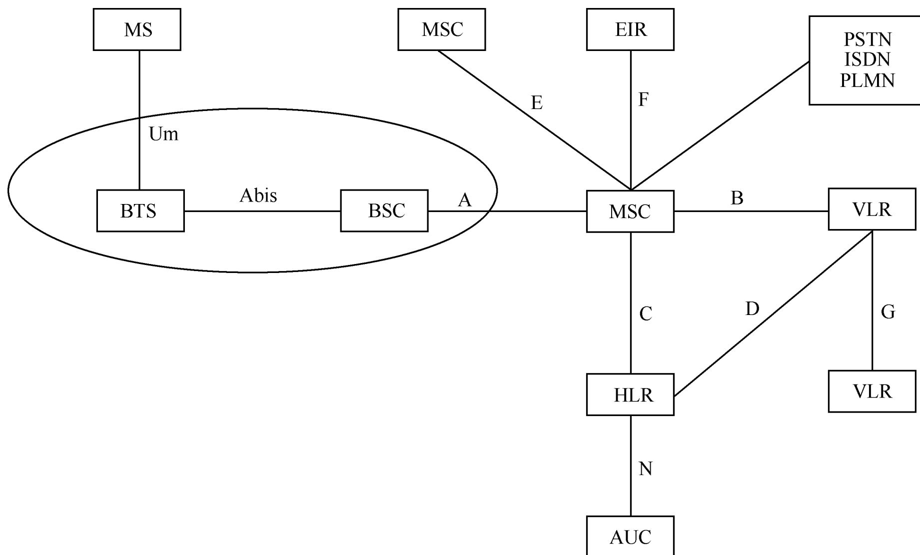


图 8.1　GSM 网络接口

我们在 4.3 节已经对这些接口作过简单的介绍，现在要关注的是这些接口的功能。然后把讨论的重点放在图 8.1 圆圈所示部分，即 Um 接口、Abis 接口、A 接口，这是我们进行信令分析用得最多的 3 个接口。对于这 3 个接口，介绍其物理层、数据链路层和网络层是有必要的；对于其他接口，我们一笔带过。

1. Um 接口

Um 接口是 MS 与 BTS 之间的接口，是手机与网络的唯一通道。有人或许就要疑惑了，这个 MS 既然只与 BTS 有接口可以通信，那么 MS 又怎样与 BSC 和 MSC 完成信令交互呢？要知道 BSC 和 MSC 都有指令要发给 MS 的，这时候，我们就可以把 BTS 当作一个传令兵、中转站，它把 BSC 和 MSC 想发给 MS 的指令不加修改地也不作处理地转交给 MS，我们也把这种方法称为 DTAP（Direct Transfer Application Part）。

Um 接口的物理层建立在无线信道上，为了满足完成不同的工作任务的需求，我们设计了各种各样的逻辑信道，分为广播信道、通用信道和专用信道等几类，这一点在第 5 章中已经对其进行过讨论。

Um 接口的数据链路层为 LAPDm，这个协议并不新鲜，它是在固定网 IDSN 的 LAPD 协议基础上稍加修改而形成的。这么偷懒是有道理的，电信网从整体而言，还是一个相

对封闭的系统，设计任何一种协议也好，设备也罢，都要注意和已有体系的后向兼容和前向演进，应当说是非常注重传承的，在这一点上与互联网有很大的不同。

Um 接口的第三层信令包含了无线资源管理（RRM）、移动性管理（MM）和连接管理（CM）3 个子层，第 6 章中对这 3 个子层进行了详细的分析。下面通过图 8.2 来看看这 3 个子层在 GSM 设备里的应用。

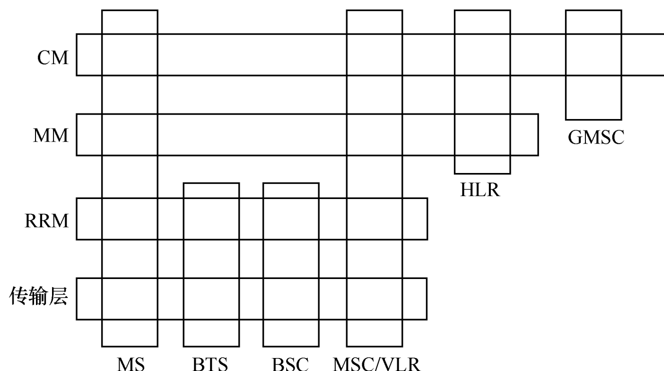


图 8.2　RRM 子层、MM 子层、CM 子层在 GSM 网络里的应用

从图 8.2 中可以看出，这就是所谓的术业有专攻啊！BSC 和 BTS 只关注 RRM 的内容，只知道修路，逢山开路，遇水搭桥，相当于军队建制里的舟桥部队，其作用就是保证通信道路的畅通和质量。路是修好了，可是道路上的物资和部队如何进行运输和调度，舟桥部队（BTS&BSC）可管不了，这个工作需要调度中心（MSC）、档案中心（HLR）通力协作，完成物资的导向和接续工作，这就是 CM 的内容；部队自然是需要进行鉴权认证工作的，以免破坏分子或者奸细混进来，然后每个小分队（MS）的位置也是需要记录的，这就是 MM 的内容。有关这 3 个子层的详细内容请参见第 6 章。

2. Abis 接口

Abis 接口是 BTS 与 BSC 之间的接口。这个接口很特殊，特殊之处在于 GSM 协议并没有给 Abis 接口以非常明确的规范，所有 Abis 接口的实现方式在各厂家之间有所不同，结果引发了一连串有意思的故事，比如“跑马圈地”和“整体搬迁”之类，具体请参见 4.3.2 节。

Abis 接口的物理层是 PCM 传输，也就是通常意义上的 2M 传输。

Abis 接口的数据链路层是以 LAPD 协议传送信息，请注意不要与空中接口的数据链路层的 LAPDm 协议弄混淆。LAPDm 是在 LAPD 协议上经过少许修改而来的，LAPD 协议可是一种很经典、很传统的数据链路层协议。

Abis 接口的第三层主要包括两部分内容：基站管理（BTS Management，BTSM）和



RRM。话说 BTSM 都干些什么活呢？首先是要管理信道，比如 BCH（广播信道）、CCH（控制信道）、DCCH（专用控制信道）；其次当然是要传递第三层协议，比如 MM 和 CM，当好一个二传手，对 MS 与 MSC 之间的信令完成一个转手的过程。

3. A 接口

A 接口是 BSC 和 MSC 之间的通信接口，MSC 通过该接口可以实现与 BSS 系统的信令交互。

A 接口的物理层和 Abis 接口一样为 2M 的 PCM 传输。

A 接口的数据链路层基于 7 号信令系统的 MTP2 层，也就是我们上一章所说的“沙和尚完成的工作”。

A 接口的网络层由 MTP3 和 SCCP 共同组成，“八戒和猴哥共同完成调度工作”。

A 接口比 Um 接口和 Abis 接口要复杂，因为它又多了一个用户层。A 接口的用户层传递的是 BSSMAP（Base Station Subsystem Management Application Part，基站子系统管理应用部分）和 DTAP（Direct Transfer Application Part，直接传送应用部分）。DTAP 主要包括 MM 和 CM。在这里，我们一定很好奇 RRM 跑哪里去了，因为图 8.2 中画得可是清清楚楚，MSC 管天管地管空气，什么事都要操心，RRM 的事情它也没打算都放手给 BSC，它还是要管的，所以 A 接口没有 RRM 信令，那是不可思议的事情。其实事情是这样的，RRM 信令到了 A 接口，就披了一件 BSSMAP 的马甲，好与七号信令的结构融洽相处。一般而言，BSSMAP 消息就是负责信道指配、寻呼、切换等典型的 RRM 的内容。MM 和 CM 前面说得很多，就不再重复。

4. B 接口

我们知道，VLR 相当于用户数据的临时存储器。MSC 作为呼叫控制的核心部分每次呼叫自然少不得去 VLR 里取相关的数据。由此可见，MSC 和 VLR 之间有大量的信息交互那是一定的，例如位置信息、补充业务信息、开通业务信息 MSC 都要通过 B 接口去从 VLR 里取，你说 B 接口能不超级繁忙吗？为了保证 B 接口的通信，把 MSC 和 VLR 合设在一起，B 接口也就成了内部接口。

B 接口用于 MSC 向 VLR 查询 MS 当前的位置信息（VLR 向 MSC 返回 LAI），或者通知 VLR 更新 MS 的当前位置信息，或者用于补充业务的操作。

5. C 接口

C 接口是 MSC 与 HLR 之间的接口，C 接口使用 MAP 信令。MSC 通过该接口向 HLR 查询被叫移动台的路由信息，HLR 提供路由功能，即漫游号码 MSRN。

6. D接口

D接口是HLR和VLR之间的接口，D接口使用MAP信令。它主要用于HLR和VLR之间交换位置信息和用户信息。当MS漫游到某VLR的辖区后，通过位置更新VLR就知道来了新的用户。VLR根据MS的IMSI号就知道MS属于哪个HLR，然后VLR就向该HLR索取资料："哥们，把你那里关于该MS的相关资料寄一份给我吧。"HLR收到VLR发过来的查询指令，核对一下IMSI号，找到相应的用户资料和业务信息发给VLR，好让VLR给漫游客户提供合适的业务。

事情到这里不算完，MS来到当前VLR之前是在另一个VLR里晃悠的，那个VLR里也保存了该MS的资料！这就太没有必要了，太不符合建设节约型社会的要求了！GSM规范想了一个办法来解决这个问题，那就是HLR向MS当前所在的VLR传递数据的同时，也向MS之前所在的VLR发送一个删除命令，要求该VLR把MS的数据删掉。要不你从广州一路漫游到北京，整个京广线上的城市都塞满了你的资料，你得浪费国家多少资源啊。

7. E接口

E接口是MSC与MSC之间的接口，两个MSC之间没有太多别的活干，它们之间信令的主要作用就是用于越局切换和建立呼叫接续。E接口使用TUP信令和ISUP信令。

8. F接口

F接口在中国目前就没有使用，是MSC与EIR的接口，用于检验IMEI用。EIR有一个很牛的功能那就是可以设置"黑名单"，禁止某些IMEI号入网，因为按照GSM规范的要求一台MS对应一个唯一的IMEI号。如果谁的手机丢了，只要他能提供足够的证据说明该手机的确是他的，那么他就可以去运营商报案，让运营商把该手机的IMEI号设置在"黑名单"里面，这个手机就没法入网了，不能入网的手机跟一个玩具没有什么区别。

不过因为山寨机的出现，一部手机对应一个IMEI号的规则被打破了。山寨厂家是没有ITU提供的IMEI可供使用的，那么他们生产的手机只能用正规厂家生产手机的IMEI号。之前在某国就传出这样一个新闻：某用户的手机丢了，去运营商报案，运营商理所当然就把该手机的IMEI号给锁了，这一锁不要紧，竟有几十部手机因此入不了网了。一查，这几十部手机都是山寨机，用的都是同一个IMEI号。

9. GSM与其他网络的接口

GSM系统中的GMSC（网关移动交换中心）还需要和其他网络（PLMN、PSTN、ISDN）



进行通信，这些接口一般采用七号信令。

8.1.2 Um 空中接口&Abis 接口

我们在上面对 GSM 的各个接口进行了一番概述，接下来就要在 8.1.2 节和 8.1.3 节讨论最重要的 3 个接口：Um 接口、Abis 接口和 A 接口。因为 Um 接口的数据链路层与 Abis 接口的有颇多相似之处，不妨把它们放到一起进行讨论。

Um 接口是 MS 和系统连接的接口，Abis 接口是 BTS 与 BSC 的接口，这两个接口的协议如图 8.3 所示。

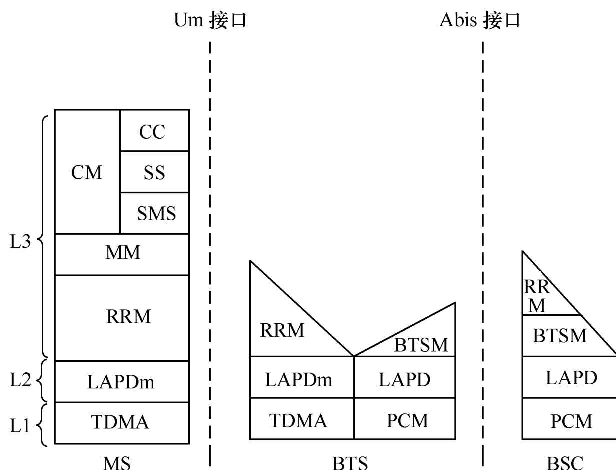


图 8.3 Um 接口与 Abis 接口的协议

我们还是采取自底向上的方式逐层进行分析。

1. 物理层

Um 接口的物理层是 TDMA 帧，我们在第 5 章已经讨论过了，就不再赘述。Abis 接口采用的是 2Mbit/s 的 PCM 线路。

2. 数据链路层

Um 接口的数据链路层为 LAPDm 协议，它是在 LAPD 协议上修改而来的。修改的目的是为了减少不必要的字段以节省开销。比如说 LAPDm 协议和通常的数据链路层协议就不太一样：一是它不需要进行定位，GSM 是采用时隙对信号进行定位的；二是它采用了卷积码进行信道编码，因此不再需要数据链路层进行信号的定位帧校验。

Abis 接口采用的是 LAPD 帧，和一般的数据链路层的帧一样，LAPD 帧是有定位和

帧校验的，有关定位和帧校验的问题也可以参见第 7 章对于 MTP-2 的描述。

首先我们来看看定位。LAPD 和 MTP-2 都是采用的 HDLC（High-Level Data Link Controller，高级数据链路控制）帧的方式，如图 8.4 所示。

01111110	内容	01111110

图 8.4　HDLC 格式

我们看到，帧头和帧尾都采用了一个“01111110”的 8bit 标志，这个标识用来区别一个信号的开始与结束。为了防止正常信号里出现这种排列方式，从而导致虚假的开始和结束，数据链路层引进了“0bit 插入机制”，具体可以参见 7.2 节。

对于 LAPDm 帧，由于空中接口可以用时隙号、保护间隔和 TA 值来对信号进行精确定位，能从时间上把信号进行分隔，所以就不再需要这个“01111110”标识来区隔信号了。

其次我们来看看纠错，纠错是数据链路层最重要的功能之一。LAPD 帧和 MTP-2 一样，是采用循环校验来进行错误的检测的。值得注意的是，LAPD 帧和 MTP-2 帧都不是采用的前向纠错，也就是说循环校验码检出的错误，它没有办法自己进行修正。而必须通过后向纠错，也就是通过发信端重复发送信号来进行纠错。我们不妨把数据看作习题，所谓前向纠错，就是在习题集的最后给了你习题答案和足够信息量的解题步骤，让你不但可以检测出答题是否正确还可以自我修正答题；所谓后向纠错就是只给了你一个孤零零的答案，你可以根据它比对出来你答题是否错了，至于怎么纠正，你得去找老师，让他给你再讲一遍。

虽说纠错是数据链路层的重要功能，然而并不是所有的 LAPD 或者 LAPDm 帧检测出了帧错误都需要进行纠错，有的帧去纠错就没有一点意义。比如说 MS 向 BTS 发送的测量报告，因为是以 480ms 为周期连续不断地向 BTS 发送测量报告，那么显然一个新的测量报告比刚才旧的测量报告有价值得多，那么如果刚才那个旧的测量报告发生了错误，对它还去浪费资源进行纠错，有必要吗？与测量报告类似的还有 SACCH 上发送的系统消息以及系统对移动台切换接入本小区的应答等，这些都不需要去进行纠错。

那么按照是否需要进行纠错我们可以把 LAPDm 帧和 LAPD 帧分成两类：一种是不需要纠错的，称为非证实模式，我管你接收端收没收到，我只传一次；第二种是需要进行纠错的，称为证实模式，可以通过重发数据来纠正这个错误的帧。

然而系统又怎么才能搞得清楚数据链路层当前是处于证实模式还是非证实模式呢？我们可以采用如下方式在接口的两端启动一个证实模式的传输：设置两条消息，为 SABM（设置异步平衡模式）和 UA（无编号证实），发端发出一条 SABM 帧，收端回送一条 UA 帧，这么一来一往两边的计数就同步了，就正式进入了证实模式的状态。证实模式是需要纠错的，纠错显然需要发端和收端都准备好，收端发现错误要及时通知发端，发端要及时重发，那么通过一来一回两条消息让双方都进入状态显然是必要的。其实在日常生



活中我们也通过这种双方一来一回的方式来表示进入另一种状态，比如拍摄现场，导演举起手中的牌子，对着演员大喊“Ready”，这算是一条 SABM 帧，通知演员进入状态，演员通过眼神或者动作告诉导演我已准备完毕，这算是一条 UA 帧回应。这样就进入拍戏状态了，之前可以没心没肺嘻嘻哈哈，接下来就得跟着戏走，不能出错了。

当要释放已建立的证实模式的时候，可通过使用 DISC 帧和 UA 帧的消息对来释放所占的资源。这就好比戏拍完了，导演喊“过”，就好比给演员发送一条 DISC 帧，告诉她戏可以结束了；演员冲导演甜美一笑，就好比一个 UA 帧，拍戏状态就此终止。

下面我们来介绍一下 LAPD 和 LAPDm 使用的帧类型，共有 3 种不同的类型，它们分别为 I 帧（编号消息帧）、S 帧（监督帧）和 U 帧（无编号信息帧并有控制功能），如表 8.1 所示。

表 8.1　　LAPD 和 LAPDm 帧类型（其中 RNR 和 FRMR 在 LAPDm 中不用）

类　型	帧	含　义	作　用
U 帧	SABM	设置异步平衡模式	建立证实模式的第一个帧
	DISC	断开	释放建立模式的第一个帧
	UA	无编号响应	对上面两类帧进行响应
	DM	非连接方式	指示非连接模式的响应
	UI	无编号信息	信息帧（非证实模式）
I 帧	I	信息	信息帧（证实模式）
S 帧	RR	接收准备好	“可以继续”（流量控制），用于肯定回答
	RNR	接收未准备好	“应该停止”（流量控制）
	REJ	拒绝	否定回答
	FRMR	帧拒绝	向回报告差错

S 帧很大程度上是用于流量控制的，流量控制也是数据链路层一个重要的功能。它可以采取 RNR“停”和 RR“走”两种模式来对流量进行控制。

话说信息帧用于传递信息，可是信息帧却有多种，以 Um 口为例，就有信令和短消息业务两种，怎么来区分它们呢？我们在 4.5.2 节中讲过类似的案例。在那节中，BTS 公司的总经理——主控板先生通过 TEI 标签来区分上级发给劳模 CTU 的指令和发给自己的指令。我们在这里如法炮制，用一个叫 SAPI（Service Access Point Indicator，业务接入点识别符）的标签来进行区分信令和用户的短消息。我们这样定义，SAPI=0 是对应着信令；而 SAPI=3 是对应着短消息业务。

Abis 接口就显得稍微复杂一些，它首先得区分 3 种不同的消息，即无线信令、设备的操作和维护消息，还有链路管理消息。为了省事偷懒，咱们照抄 Um 接口的办法，还

是贴标签，这标签的名字也叫 SAPI，对应关系如下：SAPI=0 对应无线信令，SAPI=62 对应操作和维护功能，SAPI=63 对应第二层的管理信令。我们可以看到，和 Um 接口一样，SAPI=0 也是对应着信令，这么好记，可见设计者很厚道。

麻烦事不止这些，不同设备之间也要进行区分，比如 BTS 中不同载频就要有不同的标识，否则这些信令消息传到哪个物理实体只有天知道！这个问题在 4.5.2 节中就被主控板同学解决了，就是用 TEI（Terminal Endpoint Identifier）来对其进行区分。

LAPD 和 LAPDm 帧的结构如图 8.5 所示，请注意了，LAPDm 帧中是没有 FCS 字段和 Flag 字段的，其原因在上文中已经说过了。



图 8.5　LAPD 和 LAPDm 帧结构

3. 网络层：Um 接口的第三层协议和 Abis 接口的 BTSM

（1）对于第三层协议，我们应该并不陌生。第 6 章中已经对 RRM、MM 和 CM 进行了详细的分析。在这里，我们只对第三层协议进行一番简单的总结。

Um 的网络层中包括了 RRM、MM、CM 这 3 个子层，这 3 个子层以公司的部门作为类比的话，那么 RRM 和 MM 就属于支撑序列的部门，CM 就是业务部门。RRM 就是后勤部，其职责是后勤保障，修路搭桥，保证畅通；MM 就是安全保卫部门，其职责是人员位置登记的管理和人员的鉴权管理。这两个部门的职责都比较单一。而 CM 层就要复杂了许多，业务部门做大了就难免要细分，比如电信和联通的业务部门就不约而同地分为市场部、个人客户部、家庭客户部、集团客户部。而 CM 层根据业务内容的不同也分为呼叫控制（Call Control，CC）、补充业务（Supplementary Servies，SS）管理、短消息业务（Short Message Service，SMS）。其中，CC 用于提供并行呼叫处理能力，SS 用于提供补充业务功能（比如呼叫转移、呼叫等待），SMS 用于短消息处理。无线 Um 接口第三层协议如图 8.6 所示。

我们之前说过，在 LAPDm 帧中，可以通过 SAPI 标签来区分短消息和信令。问题



是，RRM、MM、CM 这 3 种消息通通属于信令，其 SAPI 都是等于 0，SAPI 这个标签在这里失效了，没法区分它们，咱们得想办法弄一个新的标签。

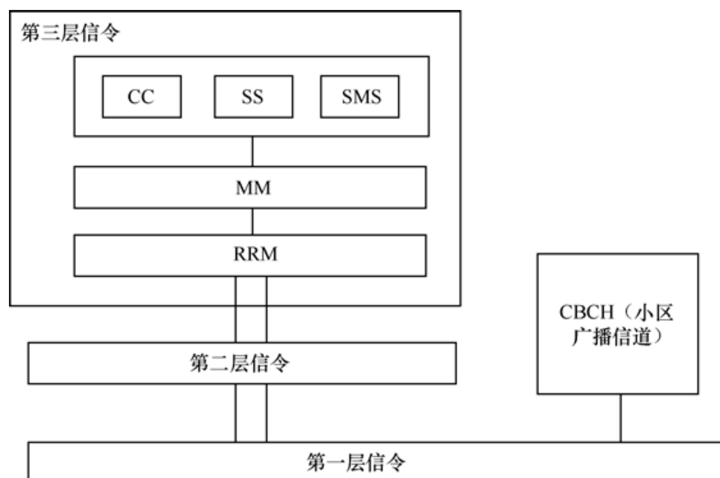


图 8.6　无线 Um 接口第三层信令结构

在这里，我们引入一个协议鉴别器（Protocol Discriminator，PD），信源发 RRM、MM 等各种消息的时候就把 PD 标签“啪”地一下贴到消息的身上，我们就可以把它看成消息的一部分。BSC 先是看 SAPI 标签，一看 SAPI=0，就知道这是一条层 3 信令，然后就要判断到底属于哪一类信令，是 RRM 还是 MM，亦或是 CM?

接下来它就去看 PD 标签，根据 PD 判断是哪类消息，如果是 RRM 消息，则在它本身处理；若为 MM 消息或 CM 消息，则送至 MSC；MSC 根据 PD 将其送至合适的软件处理单元。

PD 标签可以用于区分大部门，你到底是后勤部的，还是安全保卫部的，亦或是市场部的，一看 PD 就知道了。但是 PD 的能力毕竟有限，只能搞清楚大部门，遇到 CM 这种大部门里还分小部门的，它就傻眼了。一封信（信令消息）到底是给个人客户部的，还是家庭客户部的，亦或集团客户部的，PD 那是丈二和尚摸不着头脑，无奈啊，它不得已又找了一个帮手，这个帮手的名字叫做 TI（Transaction Identifier，事务处理标识）。

你协议鉴别器 PD 不是没法区分 CC（呼叫控制）和 SS（补充业务）吗，那好，你架不住我在 CC 和 SS 脑门上再贴一个标签——TI，我一路标签贴下去，就不信我分不清谁是谁。TI 由发送端插入（MS 或 MSC），接收端（MS 或 MSC）可以根据收到的 PD 和 TI 将消息分配到合适的地方。

上面我们都是从宏观的角度介绍了一下 RRM 消息、MM 消息和 CM 消息，下面换成微观的视角，列一列表（表 8.2、表 8.3 和表 8.4），看看这项消息都有哪些项目。列举这些消息的目的是为了让读者对 3 种信令消息有一个清晰的认识，为了达到这个目的，我们只需要勾勒出信令消息这幅场景中最关键最重要的轮廓，而无需像工具书一样面面

俱到。打仗要有重点，什么是重点，集中力量撕裂这一处你就可以通过这个缺口推进到纵深，从而扯开整条防线，那这里就是重点；读书也要有重点，什么是重点，读透这些地方就可以将你引向深入从而形成对一门学科的整体认识，那它就是重点。我们无需去纠缠每一个细节，对每一个环节平均使力是不值得的。

表 8.2　　RR 消息类型

类　别	消 息 名 称
信道建立消息（Channel establishment messages）	立即指配（Immediate Assignment）
	立即指配拒绝（Immediate Assignment Reject）
加密消息（Ciphering messages）	加密模式命令（Cipher Mode Command）
	加密模式完成（Cipher Mode Complete）
切换消息（Handover messages）	指配命令（Assignment Command）
	指配完成（Assignment Complete）
	指配失败（Assignment Failure）
	切换接入（Handover Access）
	切换命令（Handover Command）
	切换完成（Handover Complete）
	切换失败（Handover Failure）
	物理信息（Physical Information）
信道释放消息（Channel release messages）	信道释放（Channel Release）
寻呼消息（Paging messages）	寻呼请求消息 1～3（Paging Request1～3）
	寻呼响应（Paging Response）
系统信息消息（System information messages）	系统消息 1（System Information 1）
	系统消息 2（System Information 2）
	系统消息 3（System Information 3）
	系统消息 4（System Information 4）
	系统消息 5（System Information 5）
	系统消息 6（System Information 6）
	系统消息 7（System Information 7）
	系统消息 8（System Information 8）
杂项消息（Miscellaneous messages）	信道模式修改（Channel Mode Modify）
	信道模式修改证实（Channel Mode Modify ACK）
	信道请求（Channel Request）
	测量报告（Measurement Report）



表 8.3　　　　　　　　　　　　MM 消息类型

类　　别	消 息 名 称
登记消息（Registration messages）	IMSI 附着指示（IMSI Attach Indication）
	IMSI 分离指示（IMSI Detach Indication）
	位置更新接收（Location Update Accept）
	位置更新拒绝（Location Update Reject）
	位置更新请求（Location Update Request）
安全消息（Security messages）	鉴权拒绝（Authentication Reject）
	鉴权请求（Authentication Request）
	鉴权响应（Authentication Response）
	识别请求（Identity Request）
	识别响应（Identity Response）
	TMSI 再分配命令（TMSI Reallocation Command）
	TMSI 再分配完成（TMSI Reallocation Complete）
连接管理消息（Connection management messages）	CM 业务接收（CM Service Accept）
	CM 业务拒绝（CM Service Reject）
	CM 业务请求（CM Service Request）

表 8.4　　　　　　　　　　　　CC 消息类型

类　　别	消 息 类 型
呼叫建立消息（Call establishment messages）	提醒（Alerting）
	呼叫证实（Call Confirmed）
	呼叫进程（Call Proceeding）
	连接（Connect）
	连接证实（Connect ACK）
	紧急建立（Emergency Setup）
	进展（Progress）
	建立（Setup）
呼叫信息状态消息（Call information phase messages）	修改（Modify）
	修改完成（Modify Complete）
	修改拒绝（Modify Reject）
	用户信息（User Information）

续表

类　别	消息类型
呼叫清除消息（Call clearing messages）	拆链（Disconnect）
	释放（Release）
	释放完成（Release Complete）
杂项消息（Miscellaneous messages）	阻塞控制（Congestion Control）
	通报（Notify）

我们在本书中已经反复强调，RRM 要义在于建立和维护好一条自 MS 至 MSC 的无线链路。但是怎么才能完成好这一项任务，的确是件费思量的事情。就好比对于舟桥部队的指挥官而言，怎样快速建好并维护好一条通道是件很需要花大心思的事情。

首先，本着负责任的态度，你不能光顾着修路，你得向周围形形色色的车流和人流通知路况信息，因为你的终极目标是让大家顺利到达目的地，你不是为修路而修路。要不然你桥修好了，大家不明路况，一拥而上把你所修的桥挤塌了那就尴尬了。所以 RRM 的第一项工作就是广播路况，这就是“系统消息”的作用。“系统消息”告诉 MS 有哪些频点可选，比如什么 112、686，就好比路况信息告诉你到达目的地有哪几条国道可选，“112 国道”、“686 国道”；不仅如此，位置区信息也得告诉你，LAC 号、CI 号一样都不能少，免得你搞不清身在何处；光有上述两点，可算不得完整的路况信息，它显然得告诉你一系列参数让你好决定选择哪条道路，这便是“小区选择参数”的用处；除此之外，与普通道路不同的是话务的道路资源很紧张，而大家打电话又没有开车在拥挤的道路上那么有耐心，那么随机接入信道（RACH）就是相当有必要的了。上述信息都包含在系统消息 1～8 中，更多的我们就不一一列举了，请参见第 6 章。

路况信息播报完了，各个 MS 都根据自己的判断选择了合适的道路（小区），现在它们想上高速了（接入系统）。想上高速可以啊，麻烦您先去入口领通行证吧（杂项消息—信道申请），我们前面说了，这条话务高速上资源很紧张，不是谁的请求都会被批准的，要是批准了，就会给你一条“立即指配”指令，不行的话就“立即指配拒绝”了。允许你上路了这还没算完呢，话务高速可不像咱普通的高速一样每条道一般宽窄，为了节省资源，这路可是有宽有窄，你刚上路，谁也不知道你这车到底哪条路合适，就先给你分配一条最窄的路（SDCCH 信道）。然后系统会根据你的各项信息评估一下你是否需要一条更宽的路（TCH 信道）。如果要换道路，就会“信道模式修改”，更改你的道路信息，然后就要下发“指配命令”，指配 TCH 信道了。

这 TCH 高速与普通高速还有一点不同，那就是普通高速一般路况不会突然变坏，但 TCH 高速就如“六月的天气孩子般的脸”，说变就变，一旦状况恶化得不行了，就得换



条路，这就是“切换接入”及其相关信令的作用。怎么就知道一条路的状况不行了呢，那得靠“测量报告”。

除此之外，我们发现 RRM 连加密都算上了，真可谓服务到家了。说起这运输玩加密，这灵感还真来自青面兽杨志，杨志押运生辰纲可谓机关算尽啊，金银财宝上面都堆满了一袋袋的红枣用以伪装，算是一种很不错的加密了，只可惜还是被吴用给破解了。

上面一系列的步骤环环相扣，终于才算把运输这回事搞定，这 RRM 的活不轻松啊。

RRM 连接建立之后，接下来就是 MM。MM 的主要任务是两项，一项是记录移动台的当前位置以及开关机状态，知道了移动台的位置和状态，该移动台成为被叫时就知道去哪个区域找它，要不要找它（关机了自然不用去寻呼它）这便是“登记消息”的要义；另一项工作是对移动台进行鉴权，判别它是否是合法用户，这便是“鉴权请求”；如果是，则可以分配一个 TMSI 号用以作为用户的 IMSI 号的替代号，使得安全性更有保障，这便是“TMSI 再分配”。当然，你可以用 TMSI 号去鉴权，也可以用 IMSI 号，如果 TMSI 号鉴权不成功的话，那么系统就会发出“识别请求”，要求移动台提供 IMSI 号。连接管理消息算是 MM 和 CM 的接口，MM 层的工作完成了，就得向 CM 层请求工作了，这就是“CM 业务请求”。

下面我们不妨就来介绍一下 CM 子层最主要的组成部分——CC（Call Control，呼叫控制）消息，见表 8.4。

建立好了自 MS 至 MSC 的信令通道，对位置和安全性进行了管理之后，鸣锣开道的事情做完了，就该我们的 CM 出场了。

“呼叫建立消息”完成的都是一些传统程控呼叫的流程，我们在后面进行主被叫分析的时候都会用到，就不在这里展开。“呼叫清除消息”也很自然，电路可是很贵的，电话打完了这条道自然不能还被占着，得安排一些流程来清除它。“呼叫信息状态消息”用于改变一个呼叫的负载能力，在网络层与数据链路层相似的地方是也有“阻塞控制”，用于控制流量。

我们上面对 RRM、MM 和 CM 的消息进行了列举，这三者还有所不同。RRM 的主要工作就在 BSS 系统里，偶尔需要与 MSC 打交道。而 MM 子层和 CM 子层则完全不在无线子系统 BSS 里进行分析，这些消息 BTS 和 BSC 都不加分析地直接扔给 MSC。位置、安全和呼叫的控制都不是 BSS 的事情，它只需要负责牵线搭桥，做一苦力就可以了，但是这桥搭得壮不壮实，够不够宽就是它的事情了。

（2）Abis 接口的基站管理（BTS Management，BTSM）层。

关注完 Um 接口的第三层之后，让我们下面来讨论一下 Abis 口的第三层——BTSM，BTSM 用于支持分配传输路径和测量报告处理，其承载方式是 LAPD 信令协议。Abis 接

口的 BTSM 分为以下 4 个子层。

① 无线链路层管理（RLM，Radio Link Layer Management）。RLM 子层消息用于 BSC 控制 LAPDm 的连接，大多数无线接口上的层 3 信令都通过该子层进行传送。

② 专用信道管理（DCM，Dedicated Channel Management）。DCM 子层对专用信道 DCCH 进行管理和分配，这些消息包含信道激活、信道释放、功率控制、加密、测量结果和模式改变等。

③ 公共信道管理（CCM，Common Channel Management）。CCM 子层对公共信道 CCCH 进行管理和分配，这些消息包含 Paging 消息、BCCH 系统消息、信道释放、立即指配命令。

④ 无线收发器管理（TRXM，TRX Management）。TRXM 子层对无线收发信机进行管理，该层消息只在 BTS 和 BSC 之间传送。

上述 4 类消息的分工不可谓不明确：RLM 负责维持路况，保证第二层工作正常；DCM 和 CCM 干的显然是 RRM 的活，这都是建立和维护一条自 MS 至 MSC 的链路必不可少的环节；至于 TRXM，就是对硬件的管理了，大家都去关注上层建筑，总得有人关注经济基础吧，硬件要是工作都不正常，拿什么去支持 RRM、MM 和 CM 呢？

我们看到了 Abis 接口的网络层也遇到了和 Um 接口的层 3 协议一样的问题，那就是第三层有若干个协议，这该如何区分呢？Um 接口通过引进一个协议鉴别器来区分 RRM 消息、MM 消息和 CM 消息。Abis 接口也如法炮制，引进了一个消息鉴别器（Messages Discriminator，MD）来区分以上 4 类消息。

8.1.3 A 接口的协议

对于 A 接口的 MTP-1 至 MTP-3，以及 SCCP 层和 TCAP 层，我们都在第 7 章里有过详尽的描述。本小节中要关注的是应用层。

A 接口在用户部分上传送的是 BSSAP 协议，BSSAP 消息又分为 BSSMAP 消息和 DTAP 消息，这两者的主要区别是 BSSMAP 消息需要 BSC 进行内部处理，而 DTAP 消息是完成从 MS 到 MSC 的直接传递功能，BTS 和 BSC 仅做转发，不做处理。深入本质来探讨，BSSMAP 消息是 MS 层 3 信令中的 RRM 消息在 7 号信令中的映射，BSSMAP 的主要工作就是完成 RRM 功能；而 DTAP 消息是 MM 消息和 CM 消息在 7 号信令中的映射。A 接口的协议如图 8.7 所示。

很不幸，我们又遭遇了和 Um 接口以及 Abis 接口同样的问题，某一层的协议不止一个。我们如何来区别 BSSMAP 消息和 DTAP 消息呢？BSSMAP 消息和 DTAP 消息设置了一个“鉴别参数”，是一个 8bit 的数据，用于区分这两种协议。其中鉴别参数为 0 说明是 BSSMAP 消息，为 1 说明是 DTAP 消息，如图 8.8 所示。



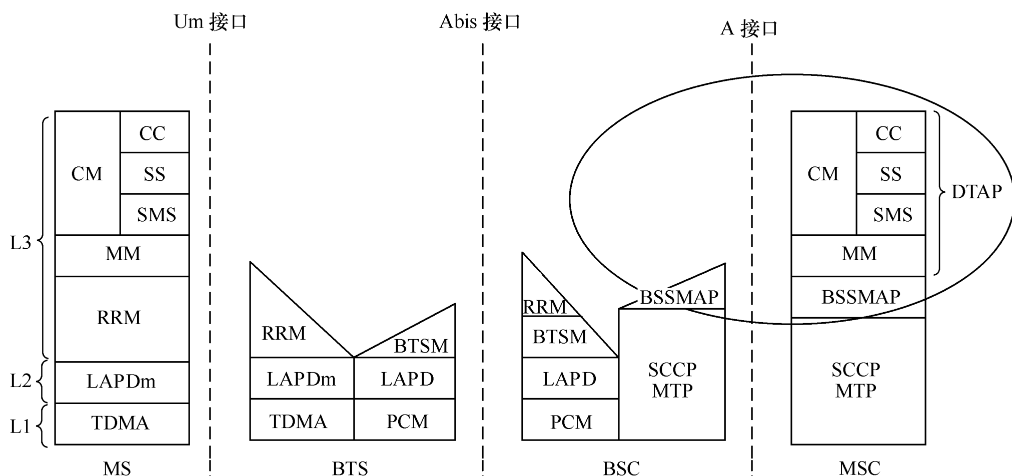


图 8.7　GSM 的 A 接口信令

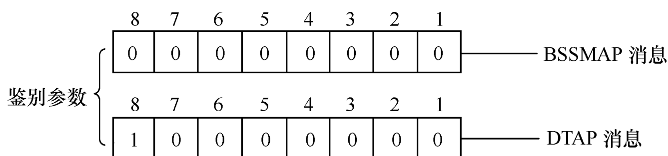


图 8.8　BSSMAP 和 DTAP 的鉴别参数

1. BSSMAP

我们首先要记住，BSSMAP 消息的大部分内容其实质就是 RRM 消息，与第 6 章的内容是息息相关的，才好理解 BSSMAP 的内容。很多人看见 BSSMAP 和 RRM 有很多相同的地方，脑子里就开始打架，其实这就是一码事，不过换了一件马甲而已。

BSSMAP 消息又分为两类。

第一类仅仅用于“MSC-BSC”之间，跟 RRM 没有什么关系，纯粹是用于 MSC 和 BSC 两个设备的管理以及查询一些东西。说起管理，无非两方面，一是陆地电路（2M 电路）的管理，二是设备本身的管理，如重启动 MSC 或 BSC 的消息。查询是指 MSC 对 BSC 资源的查询，该类消息信息量不大，采用无连接的 SCCP 消息发出。说起来这一类消息与 BTSM 管理消息中的 TRXM 消息还真比较类似，都是对硬件层面的管理，我们在前面用经济基础和上层建筑类比了这类消息与 RRM、MM 和 CM 之间的关系。

第二类则与专用信道紧密相联，属于典型的 RRM 消息，用于在专用信道上初始化 MS 消息、指配无线信道 TCH 消息、发送切换消息、发送用于专用信道释放的消息。这两类消息如表 8.5 和表 8.6 所示。

表 8.5　　BSSMAP 消息（无连接消息——管理消息）

类　　别	消　息　名	传递方向	功　　能
电路管理（Circuit Management）	阻塞（BLOCK）	BSC 到 MSC	向 MSC 指明特定的陆地资源阻塞
	阻塞证实（BLOCKING ACKNOWLEDGE ）	MSC 到 BSC	指明相关电路中的业务已经被移去
	解闭（UNBLOCK）	BSC 到 MSC	指明特定的陆地资源可恢复服务
	解闭证实（UNBLOCKING ACKNOWLEDGE）	MSC 到 BSC	指明相关电路以恢复业务
	复位电路（RESET）	双向	检测到电路异常，要求复位
	复位电路证实（Reset Circuit ACK）	双向	清除电路业务，使之空闲完成复位
MSC&BSC 管理	复位（Reset）	双向	指明发送方发生了故障
	复位证实（Reset ACK）	双向	向发送方回送应答
	过载（Overload）	双向	表明发送方过载
资源管理	资源请求（Resource Request）	MSC 到 BSC	MSC 查询 BSC 当前资源情况
	资源指示（Resource Indication）	BSC 到 MSC	BSC 响应资源请求消息

表 8.6　　BSSMAP 消息（面向连接消息）

类别	消　息　名	传 递 方 向	功　　能
指配命令	指配请求（Assignment REQ）	MSC 到 BSC	请求 BSS 指配无线资源含 Abis 口陆地电路
	指配完成（Assignment Complete）	BSC 到 MSC	所指配的请求已正确完成
	指配故障（Assignment Failure）	BSC 到 MSC	指配过程中出现故障指配已终止
切换	切换请求（Handover Request）	MSC 到 BSC	某 MS 要切换到该 BSS 所属的小区
	切换要求（Handover Required）	BSC 到 MSC	告知 MSC 要切换到的小区
	切换请求证实（Handover Request ACK）	BSC 到 MSC	BSC 成功给切换的 MS 分配信道后通知 MSC
	切换命令（Handover Command）	MSC 到 BSC	包含 MS 要切换到的目标信道
	切换完成（Handover Complete）	BSC 到 MSC	指出正确的 MS 已成功接入小区
	切换失败（Handover Failure）	BSC 到 MSC	指出在对资源分配过程中出现故障已放弃切换
	切换请求拒绝（Handover Required Reject）	MSC 到 BSC	指出 BSS 要求的切换未能执行



续表

类别	消　息　名	传 递 方 向	功　　能
切换	切换检测（Handover Detection）	BSC 到 MSC	BSC 通知 MSC 它已检测到切换接入消息
寻呼	寻呼（Paging）	MSC 到 BSC	使寻呼在正确的时间和正确的小区发送
清除命令	清除请求（Clear Request）	BSC 到 MSC	向MSC指出BSS希望释放的相关资源
	清除命令（Clear Command）	MSC 到 BSC	指示 BSS 释放相关资源
	清除完成（Clear Complete）	BSC 到 MSC	BSS 通知相关专用资源已释放
杂项消息	加密模式命令（Ciphering Mode Command）	MSC 到 BSC	要求更新相关的 MS 的加密参数
	加密模式完成（Ciphering Mode Complete）	BSC 到 MSC	MS 已更新加密参数
	完成 L3 消息（Complete L3 Informaion）	BSC 到 MSC	SABM 帧上 MS 发出的第一个层 3 消息的完成

或许有人要问，表 8.6 中的复位（Reset）和电路复位有什么区别，区别就在于一个是电路层面的复位，一个是整个 MSC&BSC 全局层面的复位。

复位：当 BSC 检测到自己严重的全局故障，则向 MSC 发送一条 Reset 消息，在等待 MSC 应答的同时，将本地标记为闭塞的电路通过闭塞地面电路或闭塞地面电路群过程通知 MSC。MSC 收到消息后，释放所有的呼叫以及相关的信息，在一定的时间之后，回送消息 Reset ACK 作为应答。

当 MSC 出现故障时，流程与上面完全一样。

电路复位：当 BSS 决定闭塞 A 接口的某条地面电路，则发送一条 BLOCK 消息给 MSC，MSC 作相应处理后以一条 BLOCK ACKNOWLEDGE 消息作为应答。当 BSS 决定解闭 A 接口的某条地面电路，则发送一条 UNBLOCK 消息给 MSC，MSC 作相应处理后以一条 UNBLOCK ACKNOWLEDGE 消息作为应答。

当 MSC 发送电路复位消息时，流程与上面完全一样。

这些内容或许有点晦涩，我们也可以这样理解，MSC 和 BSC 是两个火车站，那么电路就是联系两者的铁路。对火车站的管理和对铁路的管理自然都是必不可少的内容。如果 BSC 这个火车站出现了严重故障，它显然有必要让 MSC 这个火车站知道，要不然还照常车来车往那不乱套了，那么它就向 MSC 火车站发送“复位（Reset）”消息，并且把因为本火车站出了故障而没法使用的那一部分电路给“阻塞（Block）”掉，MSC 收到这条信息，一看，噢，你那里有麻烦了，这些线路不要再发车了，那 MSC 就把相应的车次取消掉，同时回一个“阻塞证实（BLOCKING ACKNOWLEDGE）”给 BSC，告诉

对方“哥们，你放心好了，你交代的事情办好了”。如果故障恢复了，那么车次（电路）显然也得恢复，大批的乘客（信息）还等着传递呢。这个时候 BSC 火车站就向 MSC 发送“解闭（UNBLOCK）”消息，那意思就是一切正常了，赶紧恢复运营吧，MSC 当然高兴了，也回应一个“解闭证实（UNBLOCK ACKNOWLEDGE）”，把喜悦的心情传递给 BSC“知道啦，这就组织客运”。

资源查询就更好理解了，要对全网进行管理，资源的使用情况肯定得心里有数，要不然就没法进行管理了，这当然是 BSSMAP 管理消息中的重要一环。

面向连接的 BSSMAP 消息就是典型的 RR 消息，请读者与表 8.2 对照着看，这里不再赘述。

2. DTAP

DTAP 主要用于完成移动管理消息 MM 和呼叫控制消息 CC，我们之前说了，这相当于 Um 接口层 3 信令 MM 和 CM 在 7 号信令上的映射。

DTAP 携带的消息不需要 BTS 和 BSC 解释而直接在 MSC 与 MS 之间传递，该协议简单地转发所有消息而不做任何修改。凡是由手机发起的消息直接传送给 MSC 的或 MSC 直接发给手机的消息均属于 DTAP 消息。

移动性管理 MM 和呼叫控制 CC 请分别参见表 8.3 和表 8.4，就不在这里重复了。

8.2 手机在通用模式和专用模式下都在干什么

我们在第 1 章里说过，移动通信系统和固定电话系统有一个很大的不同，那就是移动通信系统中的终端的位置是在不断变化的。由此引发了一系列与固定通信有别的通信流程，比如鉴权、加密和位置更新、切换等；另外，与固定通信有一条性能稳定的传输通道（电话线）不同的是，无线通信中终端与网络之间的无线环境几乎是一刻不停地在变化，为了保证通信质量的稳定，终端与网络之间必须进行大量的消息交互。

在 MS 开机的状态下，可以根据是否在进行通话把 MS 划分为两种状态：一种是空闲状态，另一种是专用状态（也就是通话状态）。空闲状态包含网络选择、小区选择、小区重选、位置更新和响应寻呼；专用状态下会出现立即指配、鉴权加密、主叫、被叫、短消息、切换、传输模式改变、信道释放、呼叫重建、无线链路故障判断和功率控制等事件。

我们首先来看看空闲模式下的 MS 都在干些什么。



当 MS 关机的时候，网络认为该 MS 处于“分离”状态，无法对该 MS 进行寻呼。你拨打该电话的时候，网络直接告诉你“您呼叫的用户已关机”。当 MS 由关机转变为开机时，MS 给网络发送一条“IMSI 附着”指令，告诉网络把自己的状态改为“附着”。这个附着的意思也就是说“我胡汉三又回来了”，可以当被叫了，要寻呼的可以寻呼了，要找我的可以找了。

开机首先要选择网络，很多手机开机就有一个图标在那里晃啊晃啊，然后有一行很清晰的字告诉你它在干吗——网络选择。这个网络选择有两层含义，一是选择你所属运营商的网络，是移动的归移动，是联通的归联通；二是选择归属的小区，你通话总得在某个小区下不是，这跟玩网游差不多，要玩魔兽，请您先选一个服务器，要打电话，请您先选一个小区。选择哪个小区是有规则的，也叫做 $C1$ 算法，其核心思想还是选 BCCH 载频信号强度最大的，因为接收电平通常就意味着通话质量，啥叫接收电平啊？你手机上信号有几格就叫接收电平，格数越多说明信号强度越高。又要选网络又要选小区，还要计算什么 $C1$ 算法，自然要费点时间，所以说开机慢实属正常。

选完小区不意味着万事大吉了，一来无线环境是一刻不停地在变化的，这一秒钟信号好的，下一秒钟天知道信号还好不好；然后你的手机还是处在不断运动中的，你要离当前所在的小区远了，自然当前小区就照顾不到你的手机了，如果有别的 BCCH 载频比当前载频的信号要强，那对不起，MS 我就要改投他门了。这就是小区重选，怎么进行小区重选也是有规则的，叫做 $C2$ 算法。

位置更新：我们第 1 章就说过，这就和你出去玩到了一个新的地方就要向老妈进行汇报差不多。儿行千里母担忧，得汇报；你这个 MS 到处晃悠，网络担心找不到你，所以你也得汇报。汇报的方式有几种，所在的位置区发生了变化，通知网络，这叫做“正常位置更新”；周期性地向网络报告所在的位置区，这叫做“周期性位置更新”；手机开机的时候如果发现位置区和关机的时候不一样，也要告知网络新的位置区信息，这叫做“IMSI Attach”。

寻呼：这个我们在第 1 章里也讲过，寻呼就是寻人启事，网络知道你在哪个位置区了，就在整个位置区扯开嗓子大喊，对你进行广播，要你回话，这就有了后面的接入。我们可以看到，这个位置更新其实质就是为了寻呼作准备的。

接下来看看专用状态下 MS 会干什么。

你被人寻呼了你想接入网络，你当主叫你也想接入网络，你想发短消息或者告知网络位置消息还是得接入网络。总之，只要你想告诉网络或者网络那头的 MS 一点什么信息，你就绕不开这一个流程——立即指配。什么叫立即指配呢，就是你根据你的需求向网络提出接入网络的申请，网络衡量衡量，考虑考虑，如果觉得合适的话就给你分配一条信道让你接入网络，这就叫立即指配。



接入了不算完啊，你是来到了威虎山，咱还得验证验证你是不是自己人，GSM 网络也是如此，虽然是给了你一条信道让你可以跟网络说上话了，但是还得验验你这个 SIM 卡是不是山寨版，是不是运营商我发行的，于是就有了鉴权。鉴权完了一般紧接着就是加密，既然是自己人，就说自己人的秘密语言，让外人听不懂的话。

刚开始接入的时候，因为不知底细，往往分配的是一条羊肠小道——SDCCH。后来不是已经接入了么，接入网络后 MS 把来意一说，咱是来做大买卖的，打国际长途啊，MSC 一乐啊，赶紧吩咐 BSC 重新分配一下，给这个 MS 搞一条高速路——TCH。从 SDCCH 到 TCH 的转变就涉及传输模式的更改，这是 RRM 的内容。

MS 在通话的过程中是不断移动的，这跟在空闲状态下没什么两样，也要考虑更换小区的问题。在空闲模式下更换归属小区叫做小区重选，在专用模式下更换小区就叫做“切换”（Handover）了。小区重选的算法叫 $C2$，切换的算法叫做 Locating，话说 Locating 的具体算法 GSM 规范并没有严格的定义，只是给了一些建议，设备厂家可以根据这些建议各行其是。Locating 的算法比起 $C2$ 是要复杂很多的，因为 Locating 不但要考虑下行信号的质量还要考虑上行信号的质量，并且还要考虑各个小区的资源情况，要考虑的多了，事情就复杂了。

下面就对这些通信流程进行逐一地解析。

8.3 小区选择与重选

小区选择和重选都是属于空闲模式的内容，空闲模式 MS 要进行下面的 4 项事件，如图 8.9 所示。

什么叫网络选择呢？通常意义上就是说选择运营商，一般情况下我们是没得选的，你买了谁的卡就默认登录谁的网络，移动的归移动，联通的归联通。我们可以试试在手机的网络选择一项里搜索其他运营商的网络，搜是能搜到的，但是你试图登录上其他运营商的网络就会被踢下来，人家的 HLR 没有对你开放鉴权，占用它的网络，想都别想。但这并不是绝对的，GSM 网络是一个全球性标准，胸怀当然要大气一点，最起码得有一点人道主义精神，什么意思呢？大家去一些很偏僻的地方玩的时候，手机有可能会遇到没有信号的情况，但是没有信号

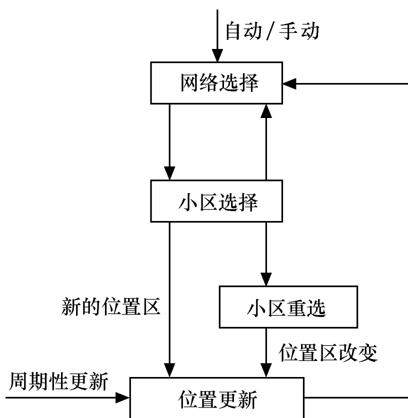


图 8.9　空闲模式下的 MS



又有两种提示：一种是“无网络”，这就说明周围没有 GSM 覆盖了，你想打电话是没办法了；另一种是“仅限紧急呼叫”，也就是你所属的运营商无网络，但是有别的运营商的 GSM 网络，在你的手机实在搜索不到所属运营商的 GSM 网络时，是可以登录别的 GSM 网络的，但是业务类型被限制了，仅仅限于拨打紧急电话，如“110”、“119”之类的。值得注意的是，哪怕你不插 SIM 卡，也是可以登录网络拨打紧急电话的，这就是 GSM 的人道主义精神，总不能说你没有 SIM 卡有紧急的事情就不让你打紧急电话了吧。

网络选择在出国漫游是有用的，比如你漫游到欧洲，一下飞机你就可以手动选择想入网的运营商，当然这些运营商得是和国内的运营商签了约的，要不人家的 HLR 还是不对你开放鉴权。欧洲的大运营商通常都与国内的两大 GSM 运营商签订了漫游协定，比如 T-mobile、沃达丰、和黄、BT、O_2 都可以随你选择。你也可以让手机自动选择运营商，通常手机是自动选择信号强度最大的运营商，这样就会带来一个问题，运营商开始竞相在机场加大基站的发射功率，以争夺国际漫游用户，为了阻止这种毫无意义的马拉松式的竞争，GSM 的设计者规定了接收的信号强度大于−85dBm（信号满格），手机就在运营商里进行随机选择，免得把机场搞成电磁辐射场。

其实国内的 GSM 网络，比如移动与联通之间，也是可以相互漫游的，在国外一部手机在运营商之间进行“异网漫游”也是比较常见的做法。不过有一个前提是进行“异网漫游”的运营商双方的 HLR 必须相互开放鉴权，因为不开放鉴权的话一个运营商的手机是无法在另一个运营商的 VLR 里完成注册的，也就打不了电话。中国移动和中国联通之间并没有达成相互开放 HLR 的协议，也就无法进行“异网漫游”。

选好了网络之后，我们下一步就是选择小区了。

8.3.1　哪家信号好我选哪家——小区选择

1. 什么叫小区选择

通常情况下，一个位置是有多个小区覆盖的（在城区尤其如此），那么 MS 就要选择一个最合适的小区，把该小区作为自己的服务小区，和该小区进行通信，如图 8.10 所示。MS 选择该小区后，就调谐到该小区的 BCCH 载频上，监听该小区 BCCH 信道广播的系统消息，以及在 CCCH 信道上接收寻呼消息。

这个过程其实与大家在学校里收听广播的过程颇为相似，大学校园里也有多个电台覆盖的，咱们也得选择一个频道作为自己的收听频道。要收听广播首先得搜索频段，搜索频段大家并不陌生，就是“吱呀吱呀”转动你那有点老掉牙的旧式收音机的旋转开关。等你调得差不多了，一个清脆悦耳的女声就从收音机里飘了出来：“91.8 兆赫，欢迎您收听湖南交通频道”，这算是调谐到湖南交通频道的“BCCH 载波”上了。交通频道播报

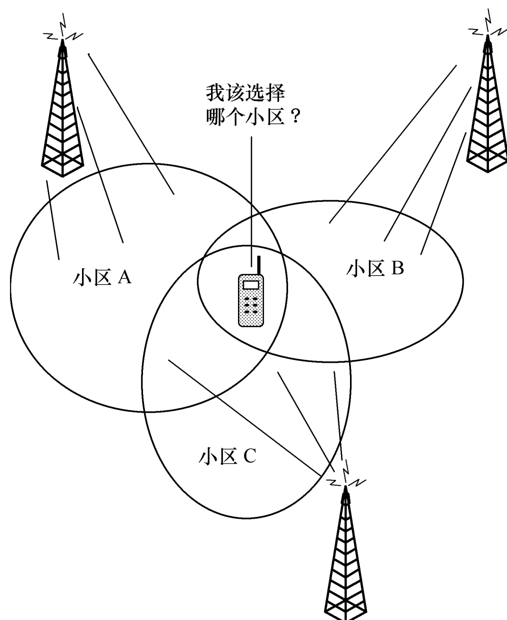


图 8.10　小区选择的困惑

的各种路况信息也就算是“系统信息”了，广播里有时候也会来个什么寻找热心的哥的寻人启事，你就只当是“CCCH 信道的寻呼消息”好了。

MS 驻留一个小区其目的何在呢？主要有以下 3 个作用。

（1）MS 从所在小区的 BCCH 载频收听系统消息，以了解网络的情况。

（2）如果该 MS 想发起一个呼叫或者发送短消息，可以通过该小区接入网络。

（3）如果网络收到一个呼叫该 MS 的消息，系统可以根据位置更新知道 MS 当前所在的位置区，然后给该位置区的所有小区向 MS 发 Paging 消息。MS 守候在该位置区的某个小区的 BCCH 载频的下行信道上，可以在该下行信道收到给自己的 Paging 消息，并通过 BCCH 载频上行的 RACH 信道回应网络对自己的寻呼。

2. MS 选择一个小区的标准是怎样的

（1）首先所选择的小区必须是所属运营商的。这个很简单，你总不能拿着沃尔玛的购物卡去家乐福买东西吧（所属运营商无网络时可以通过其他运营商打紧急电话）。

（2）其次该小区不是被禁止的。什么小区是被禁止的小区呢？这是运营商出于实际需要设置的，比如说某些小区话务量太大，那我就不希望 MS 在小区选择的时候接入该小区，从而增加该小区的负荷。那么我就设置一个 CBA（Cell Bar Access，小区接入禁止）参数。小区禁止接入由 1bit 组成，0 表示允许移动台在本接入区接入。实际上，CBA 通常与 CBQ（Cell Bar Qualify，小区禁止限制）共同组成小区的优先级状态，如表 8.7 所示。

表 8.7　小区优先级

小区禁止限制	小区接入禁止	小区选择优先级	小区重选项状态
0	0	正常	正常
0	1	禁止	禁止
1	0	低	正常
1	1	低	正常



应当说以上两个参数的用法挺麻烦的，我们举一个实际的例子来说明它的用途，如图 8.11 所示。

假设某微小区 B 与一宏小区 A 重叠覆盖一区域（见图 8.11 中阴影区）。

为了使微蜂窝 B 尽可能多地吸收 B 区的业务量（尤其是 B 区的边缘），可以设置小区 B 的优先级为“正常”，小区 A 的优先级为“较低”。这样在小区 B 的覆盖范围内无论其电平是否比小区 A 的低，只要符合小区选择的门限，移动台就将选择小区 B。

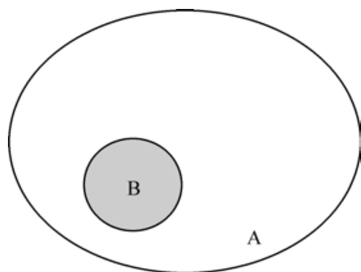


图 8.11　微小区情况下 CBQ 的应用

（3）$C1>0$，$C1$ 算法略微有点复杂，我们留待下小节再讨论。

3. MS 选择小区的流程是怎样的

MS 选择小区的流程分为两种：一种是存储了 BCCH 信息的方式，还有一种是未存储 BCCH 信息的方式。

（1）MS 存储有 BCCH 信息情况下的小区选择

一般情况下手机采用的都是这种方式，手机关机后，会把上次使用的 BA 列表（BCCH ALLOCATION）存储在手机的 SIM 卡中。

当手机再次开机进行小区选择时，将首先搜索上次关机时存储在 SIM 卡中的 BCCH 载波，如果该小区符合“2.MS 选择一个小区的标准是怎样的”所述的驻留条件，就选择该小区作为服务小区。如果不行的话，那么就从该小区曾经广播的 BA 表（Idle）里的 BCCH 频率进行搜索。

我们所说的 BA 表根据广播的系统消息的类型不同可以划分为两种：其中 BA Idle 表是通过 BCCH 信道的系统消息类型 2（系统消息我们在第 6 章里有阐述）向 MS 广播的，它包含了当前小区的邻小区，最多 32 个频点，用于小区选择和重选；BA Active 表是在 SACCH 信道上通过系统消息类型 5 向 MS 点对点发送的，其中的频点是 MS 在通话状态下测量的邻小区的频点，一共可以有 32 个频点，用于进行小区切换。

如果 BA Idle 表中所有 BCCH 载波都被搜索后，依然未能找到合适的小区驻留，那么就执行无 BCCH 信息的小区选择过程。

（2）MS 未存储 BCCH 信息情况下的小区选择

小区选择流程如图 8.12 所示。

如果移动台并无存储的 BCCH 消息，它将首先搜索完所有的 124 个 RF 频点（双频手机还将搜索 374 个 GSM1800 的 RF 信道），并且从不同的频点上抽取 5 个测试值进行平均，计算出每个频点的平均信号强度，根据不同的电平强度列出一个表，整个测量过程将持续 3～5s。

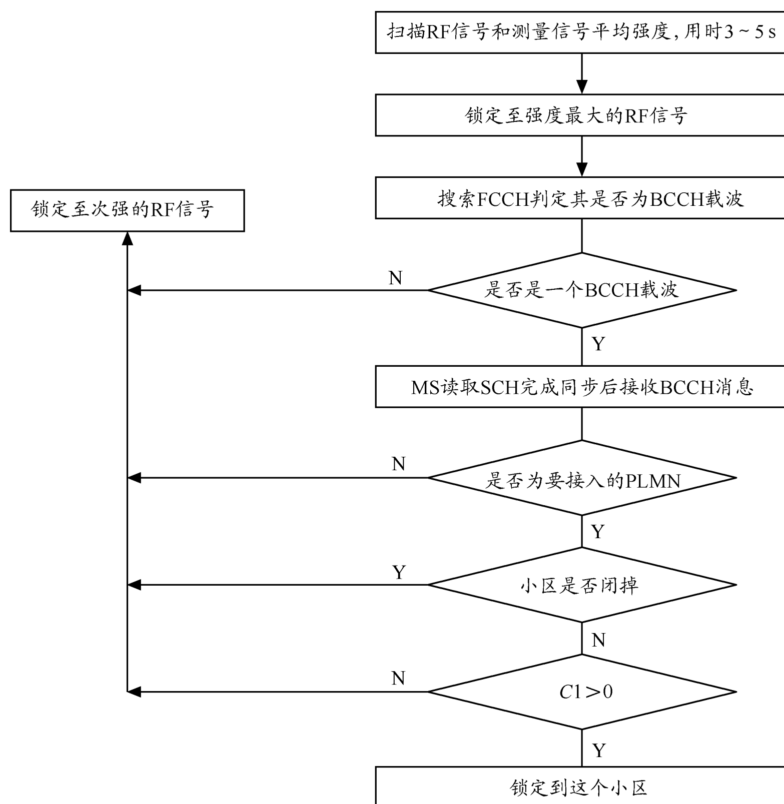


图 8.12　小区选择流程

MS 先把频率调谐到信号强度最高的频点上，然后通过检索 FCCH 突发脉冲来判断该载波是否为 BCCH 载波。如果判断是 BCCH 载波，那么 MS 将通过解码 SCH 来与该 BCCH 同步，然后读取 BCCH 上的系统消息。MS 通过解码 BCCH 上的消息，然后根据第 2 部分所述的选择小区的三大标准一条条进行判断：是否为所属运营商的网络？该小区是否已被禁止接入？$C1$ 是否大于 0？如果 3 个条件都满足，那么 MS 就驻留在该小区，否则，MS 将调谐到信号强度次高的载波上重复该过程，直到找到可用小区为止。

如果 30 个最强的 RF 信道都被搜索后仍未找到合适的小区，MS 就开始心急了。因为某个地方被超过 30 个可用信号覆盖的情况不多，信号强度排名都到了 30 位以后的小区，通话质量肯定不咋地。这时候 MS 就监测所有的 RF 信道的信号强度并搜索 $C1>0$，且未被禁止接入的小区，而不管该小区是否属于所选择的运营商。找到合适的小区后，就驻留在该频点上，不过这时候就只能进行紧急呼叫了。

上述这段文字很晦涩，或许看得一些同学哈欠连天，我们稍稍休息一下，先讲一个故事。为了吸引眼球，作者决定讲一个“**美女杜零零择偶**”的故事。



话说美女杜零零同学在海外拿了 PhD（博士学位）归来，也就是奔三的人了，就想找个对象成个家安定下来（驻留一个小区）。这又是美女，又是海归，又是 PhD 的，要求自然不会低。

她老爸先给设了两条不可违背的铁律（参见“2.MS 选择一个小区的标准是怎样的”），只能在这个框架里选。一是对方必须是本国人，因为她老爸觉得老外文化不同，不好沟通（必须是所属运营商）；二是被家长一票否决了的坚决不能要（小区接入禁止）。

杜零零同学这就开始忙活了，她首先试着寻找出国前大学男友的信息（关机时存储的 BCCH 信息），看看对方还是否合适。如果不合适，就试着联系前男友推荐给她的人（这个有点晕，指的是原 BCCH 广播的邻小区）。再没有合适的，杜零零同学就把心一横，开始进行大搜索。

杜零零首先对单位上 124 个男士进行摸底大调查，把有可能的人选按年薪多少进行排序，接下来就开始进行派对选择（小区选择），杜零零美女的选择流程如图 8.13 所示。

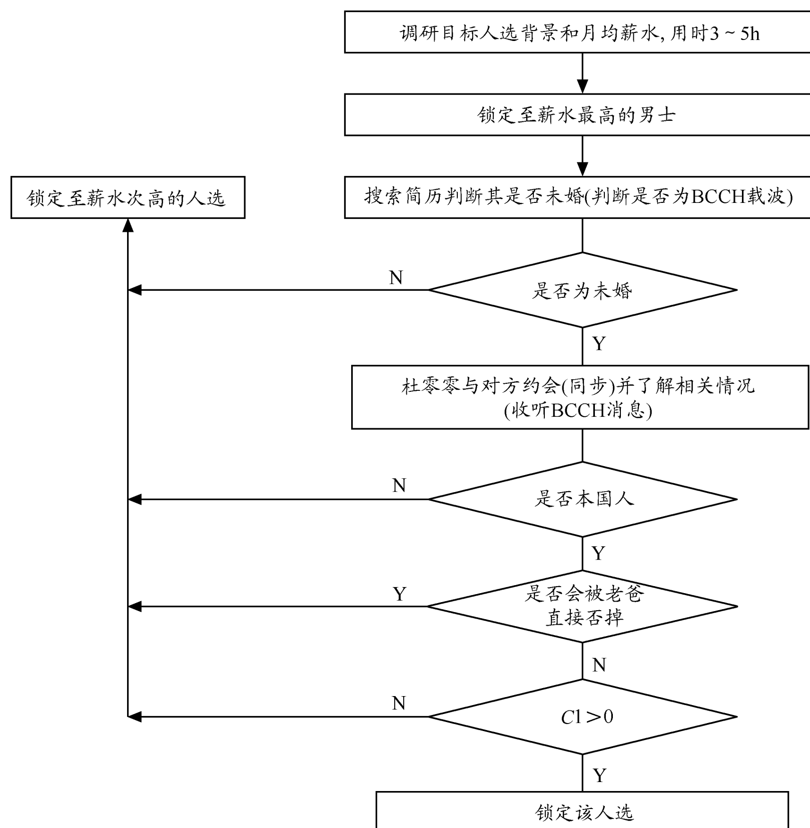


图 8.13　杜零零的选择对象流程

由图 8.13 可以看出，要娶杜零零可不容易，得过 4 道关，至于 C1 是什么呢，我们下小节再讲。这个过程可不会这样无限循环下去，刷掉 30 个候选人之后，杜零零同学就急了，俺这可是按年薪排序的，再往下找找不找得到另说，这物质条件别差得不能忍了（电平值越来越低，通话质量会越来越差）。罢罢罢，跟老爸一沟通，真到那一地步就放宽一个条件，国籍就算了（驻留到别的运营商的网络，只能打紧急电话）。

8.3.2 功率！功率！还是功率!——C1 算法三要素

我们上面说了，小区选择有 3 个需要考虑的因素：一是是否是所属的 PLMN 网；二是小区是否被禁止接入；三是 *C*1 是否大于 0。如果说前两个条件是定性的问题，那么 *C*1 就是定量的问题了，那么该如何设计 *C*1 参数呢？

我想大家在选择工作的时候心里都有一个关于薪水的底线，如果企业开的薪水高于你的底线越多，那么你就越有可能考虑加盟该企业。那么你选择企业的参数 *C*（Choice）的表达式就会如下所示：

C=企业开出的薪水−你心里的薪水底线（这个 *C* 得大于 0，否则你不会选这个企业）

那么很好，*C*1 也是这么干的，它希望 MS 的接收电平（*RxLEV*）能够比系统允许移动台接入的最小接收电平（*RxLEV_ACCESS_MIN*）要大，否则它就不选择这个小区。这个最小接收电平参数是在 BCCH 信道的系统消息 3 和系统消息 4 中进行广播的，运营商可以自行进行设置。

这就有 $C1=RxLEV-RxLEV_ACCESS_MIN$，仅当 $C1>0$ 时才会选择这个小区。

RxLEV_ACCESS_MIN 是一个非常重要的参数，这个参数的主要价值是避免移动台在接收电平很低的情况下接入系统（此时接入后的通信质量很差，以至于无法保证正常的通信过程）。对一些业务量过大的小区，我们可以通过适当提高小区的 *RxLEV_ACCESS_MIN*，从而使该小区的 *C*1 和 *C*2 变小，从而使得小区的有效覆盖范围随之缩小。

当减小该值时，将扩大小区允许接入的范围（其下限是移动台的接收灵敏度），但在边缘地带的通话质量会很恶劣，容易引起掉话，而且此时由于上行信号很弱，会导致在功率控制下的移动台以最大功率发射，从而增强上行信号的干扰。

值得注意的是，我们上面设计的 *C*1 仅仅考虑了下行，但是通信不仅有下行，还有上行的。上下行合在一起才构成一条完整的无线通路，那我们该如何考虑上行呢？

这里还是拿一个职场人选择企业为例，我们考虑薪水的时候，不仅考虑发给我们的薪水是多少（下行），还要考虑个人交多少钱给企业作为住房公积金（上行）。就我们个人的想法而言，自然是希望越多越好咯，但是当地都会有一个公积金的最高限额值 *M*，企业也有一个自身的支付能力值 *P*，有 *M* 在那里，*P* 的能力再大也受制于 *M*，但我们显然不希望 *P* 小于 *M*，*P* 小于 *M* 的话说明这个企业的福利不是很好，在我们心目中会减分



的，这样就形成了完整版的选择企业的参数。

C=企业开出的薪水−你心里的薪水底线−Max[(*M*−*P*),0]，要是企业的支付能力 *P* 大于 *M*，反正你也只能得到 *M*，后面这项不减分；要是企业的支付能力小于 *M*，那后面这个减分项就是正数了，这个企业在你心目中就要掉价了。

我们再来看看小区选择参数 *C*1，通常情况下，为了控制手机接入时对系统的干扰，都会在系统消息里规定手机接入系统时可使用的最大发射功率 *MS_TxPWR_MAX_CCH*，然后手机自身有一个最大输出功率 *P*，对于手机接入系统而言，初始功率自然是越大越好，我们希望 *P* 不小于最大允许的发射功率 *MS_TxPWR_MAX_CCH*，小于的话就要减分。那么就得到了 *C*1 的完整版公式：

*C*1=*RxLEV*-*RxLEV_ACCESS_MIN*−Max[(*MS_TxPWR_MAX_CCH*−*P*),0]



小知识

我们在上面谈到的众多参数的单位都是 dBm。dBm、dB、dBi 和 dBd 在通信中用得很多，那这几者的区别在哪里呢？下面简要讲述。

1．dBm

dBm 是一个表征功率绝对值的值，计算公式为：10lgP（功率值/1mW）。

【例 1】如果发射功率 P 为 1mW，折算为 dBm 后为 0dBm。

【例 2】对于 40W 的功率，按 dBm 单位进行折算后的值应为：

10lg（40W/1mW）=10lg（40 000）=10lg4+10lg10+10lg1 000=46dBm。

2．dBi 和 dBd

dBi 和 dBd 是表征增益的值（功率增益），两者都是一个相对值，但参考基准不一样。dBi 的参考基准为全方向性天线，dBd 的参考基准为偶极子，所以两者略有不同。一般认为，表示同一个增益，用 dBi 表示出来比用 dBd 表示出来要大 2.15。

【例 3】对于一面增益为 16dBd 的天线，其增益折算成单位为 dBi 时，则为 18.15dBi（一般忽略小数位，为 18dBi）。

【例 4】0dBd=2.15dBi。

【例 5】GSM900 天线增益可以为 13dBd（15dBi），GSM1800 天线增益可以为 15dBd（17dBi）。

3．dB

dB 是一个表征相对值的值，当考虑甲的功率相比于乙功率大或小多少 dB 时，按下面计算公式：10 lg（甲功率/乙功率）。

【例 6】甲功率比乙功率大一倍，那么 10 lg（甲功率/乙功率）=10 lg2=3dB。也就是说，甲的功率比乙的功率大 3dB。

【例 7】7/8 英寸 GSM900 馈线的 100m 传输损耗约为 3.9dB。

【例 8】如果甲的功率为 46dBm，乙的功率为 40dBm，则可以说，甲比乙大 6dB。

【例 9】如果甲天线为 12dBd，乙天线为 14dBd，可以说甲比乙小 2dB。

8.3.3 你信号不好了我就跟你说拜拜——小区重选

小区选择完了并不等于说就万事大吉了，如果周围的无线环境发生了变化或者你的位置发生了移动，导致 MS 觉得别的小区信号更好，更适合驻留，那就会导致图 8.9 所示的小区重选过程。这就好比职场，如果当前企业的待遇不行了或是别的企业能够提供更好的待遇，许多人就选择跳槽了。不过跳槽通常要考虑长期的效应，而 MS 只考虑这几秒的效应，你信号不好了，对不起，马上跟你拜拜，所以小区重选那可是件比跳槽频繁得多的事情。

小区重选是根据 MS 的测量报告来进行判断的。移动台在驻留在所选小区之后，还继续监测由服务小区的 BCCH 系统消息 2 所指示的邻小区频点配置表中的所有的 BCCH 载波，监测这个干嘛用呢？就是为了骑驴找马，随时选择信号更好的小区，有点不厚道吧，呵呵。邻区在系统消息 2 中我们知道最大可以配置 32 个，MS 不可能去对这么多小区进行跟踪解码，这也没有必要，MS 通常是选择 6 个最强的 BCCH 进行跟踪和解码，以收听它们的 BCCH 系统消息，为自己下一次跳槽做好判断。

什么时候 MS 将启动小区重选呢，也就是说什么时候 MS 就忍无可忍决定跳槽呢？

（1）小区变成禁止状态——小区不允许你接入了，开除你了，你别无选择，只能换东家

（2）在超过了最大重传次数 M 之后依然不能接入小区——身为 MS 在你小区居然 M 次都无法通过 RACH 接入网络，太伤心了，这电话没得打了，俺得换东家。

（3）下行链路误码率太高——MS 通过译码 SACCH 来判断下行链路的误码率，详见后面的内容。误码率太高说明这条链路通话质量不怎么样，早点更换小区为妙。

（4）服务小区 $C1<0$ 连续超过 5s 以上——连续 5 个月工资低于你的心里底线，你受得了吗，不忍了，跳了。

（5）另一个小区的 $C2$ 大于当前小区 $C2$ 的时间超过 5s 以上——话说这些社会学家也真够无聊的，先搞出一个什么企业选择指数 $C1$，这里又搞出一个跳槽指数 $C2$，什么是 $C2$ 呢，我们一会再谈。

（6）另一个位置区小区的 $C2$ 大于当前小区（$C2+CRH$）的时间超过 5s 以上——如果重选的小区和当前小区位置区不同，就得再加一个砝码了，即 CRH（Cell Reselection Hyseteresis，小区重选滞后），以增加跳槽的难度。因为我们知道，位置区变更是要向系



统发送位置更新信息的，你在位置区的两边跳来跳去，系统得不停地给你办位置变更的手续，换谁都受不了啊。

值得注意的是，由 $C2$ 引起的小区重选至少间隔 15s，其作用是为了避免 MS 频繁地进行小区重选，占用系统资源。另外，MS 最少每 5s 计算一次服务小区和邻小区的 $C2$ 值。

下面来研究研究这个跳槽参考指数 $C2$，看看到底是怎样构成的。

话说这个 $C2$ 虽然是社会学家搞出来的，但其实并不神秘，咱都是大俗人一个，自然明白跳槽的首要因素还是工资待遇，就是 $C1$ 那些事儿，这样我们就可以列出最初的等式：$C2=C1$。

运营商有时候希望有的小区可以吸收更多的话务，比如说希望 DCS1800 可以从 GSM900 那里吸收更多的话务，就设置一个 CRO（Cell Reselection Offset，小区重选偏置）参数来鼓励别的小区的 MS 重选到该小区来。这就是说跳槽的时候某类企业在你心目中地位更高，比如说能给你更多锻炼机会的企业，你就给这样的企业在心里的天平上加一个砝码，这个砝码就叫做 CRO，那么我们的公式就改为：

$$C2=C1+CRO$$

运营商显然是不希望小区做过频繁的小区重选的，这会浪费系统资源，因此运营商就设置一个叫 PT（Penalty Time，惩罚时间）的参数来遏制这种重选。每次重选完之后，PT 开始倒计时，倒计时之前你最好不要重选，如果一定要进行小区重选，那么对不起，请你的 $C2$ 先减去一个时间偏置 TO（Time Offset），那么 $C2$ 的表达式就变为：

$$C2=C1+CRO-TO\times H(PT-T)\text{；}PT\neq 31$$

函数 $H(x)$：当 $x<0$ 时，$H(x)=0$；当 $x>0$ 时，$H(x)=1$。等于说这个 TO 的偏置只在重选完的 PT 时间内有效，过了这个时间就归 0 了。TO 的作用是防止快速移动的 MS 进行乒乓小区重选。

这里有一个比较郁闷的地方，上面的 CRO 都是给企业的正评价，我们想给一个企业负评价怎么办。也就是说我们想降低重选到某小区的概率怎么办？

这里 GSM 的设计者为大家留了一条后路，GSM 规范规定，当 $PT=31$ 时，CRO 的符号由正变负，也就是说此时 $C2=C1-CRO$，这就达到了我们想给它一个负偏置的效果。（这样就知道为什么我们在 $C2$ 参数的表达式那里要加一个 $PT\neq 31$ 的条件了吧。）

8.4 随机接入与信道分配

话说 MS 选定了小区，接下来就是通过这个小区发起呼叫或者进行位置更新了。无



论是主叫、被叫还是短消息亦或位置更新，都必须经过随机接入信道（RACH）和允许接入信道（AGCH）的过程。之所以要进行这个过程我们在之前也讲过了，就是因为资源有限，所以不得不有控制手段。

银行的窗口总是满的，所以窗口就是稀缺资源，为了有效地管理窗口资源，银行首先采取的是要求大家排队，这是一种通用的管理手段。但后来就发现这种方式弊端不少：一是客户都必须站在那里排队，有时候一等就是半个小时甚至一个小时，腿都站酸，不太符合服务业“客户至上”的理念；二是队伍一长了还保不齐有插队的。于是后来就出了一个领取排队小票的机器，你首先按一下屏幕，算是申请办理业务了（RACH），然后机器出一个排队号的小票，算是允许你排队办理业务了（AGCH），接下来要干的活就是等着营业窗口喊你的号了。

银行并非特例，凡是资源紧张的地方，无不需要采取类似的控制手段的，比如说某些餐厅就需要预订餐桌，医院的专家教授就需要提前预约挂号。这无线通信也一样，信道是稀缺资源，不是说占用就占用的，一定得先有个申请，批准你占才能占。

在任何情况下，如果移动台要和网络建立通信，都需通过 RACH 信道向网络发送一条“信道申请”（Channel Request）的消息，这条突发脉冲只有 8bit 的有用消息，其中 3bit 用来做建立原因（紧急呼叫、位置更新、响应寻呼或是主叫请求），另外 5bit 是手机随机选择的鉴别符，它并不用来向网络提供信息，其目的是使网络能够区别不同的 MS 发送的请求。网络此后将向移动台发送立即指配指令，该命令会再将该鉴别符发给移动台，移动台通过网络返回的鉴别符和本身所发送的鉴别符相比较来判断该信息是否是网络发送给自己的。

有人或许要觉得不对，RACH 突发脉冲明明有 36bit 的信息位，在这里怎么变成了只有 8bit 的有效信息？我们来看看 RACH 突发脉冲的组成，如图 8.14 所示。

尾比特 3bit	同步序列 41bit	加密比特 36bit	尾比特 3bit	保护间隔 68.25bit

图 8.14　接入突发脉冲序列

这里有 36bit 的加密比特，这些加密比特是怎么来的呢。首先是 8bit 的信道申请消息，然后加上 6bit 的网络色码，再加上 4bit 的尾比特，就得到了 18bit，我们把这 18bit 按照 1∶2 的速率卷积，最后就得到了 36bit 的消息位。

BTS 在接到移动台的“信道申请”消息之后，就通过 Abis 口给 BSC 发送一条信道请求（Channel Required）消息，该消息包含本次接入的原因及 BTS 对传输时间（TA 值）的估计。BSC 根据接入原因和现有系统中无线资源的情况，打算选择一条空闲的 SDCCH 信道给 MS。但这条信道是否真的就可用呢，需要验证一下，BSC 于是给 BTS 发送一条信道激活（Channel Active）指令要求 BTS 激活该信道，BTS 照章办事对这条信道进行



激活，然后向 BSC 返回一条信道激活证实（Channel Active ACK）的消息来答复 BSC。

BSC 收到指令后知道该信道已经激活了，这下万事俱备，那么 BSC 紧接着就在 AGCH 信道上向 MS 发送“立即指配”消息，其中包含 BSC 分配给 MS 的 SDCCH 信道描述、接收到信道申请消息时的 TDMA 帧号、初始化时间提前量 TA 值、初始化最大传输功率以及随机鉴别符。每个在 AGCH 信道等待分配的 MS 可以通过比较自身随机鉴别符和下发的随机鉴别符，看看是否一致，从而判断是不是发给自己的消息，以避免争抢信道引起混乱。

值得注意的是，并不是所有 RACH 信道上发送的信道申请都能被分配到一条 SDCCH 信道。首先，你这申请不一定能有效送到 BTS，因为网络是有多台 MS 在运行的，完全可能因为争抢 RACH 信道让 BTS 无法有效收到你的申请。另外，信道申请消息即使送到了 BTS 并通过 BTS 转送到了 BSC，BSC 也完全有可能因为各种原因而不给你分配一条信道，比如 MSC 话务关闭、无线资源缺乏、TA 值超界等。当 BSC 没有空闲信道可供分配时，BSC 要向 MS 发出“立即指配拒绝”消息，为了避免 MS 马上又重新进行信道申请浪费系统的资源，立即指配拒绝消息可以包含一个限制 MS 继续呼叫的时间指示，该时间指示值称为 T3122 值。MS 只有等 T3122 逾时了才能重新发起信道申请。具体的内容请参见 6.2 节。

当 MS 正确地收到自己的初始分配后，根据信道的描述，就把自己调整到该 SDCCH 信道上，建立一条传送信令的链路。有了 SDCCH 信道，这仅仅是物理层建立起来了，接下来是要建立数据链路层。和其他 HDLC 协议一样，Um 接口的 LAPDm 协议也是先让 MS 发送一个 SABM 帧来建立异步平衡模式，然后 BTS 发送一个 UA 帧给 MS 作为应答，这么一来一去数据链路层就建立起来了。

不过 LAPDm 协议也有和其他 HDLC 协议不一样的地方，其他 HDLC 协议 SABM 帧和 UA 帧不用包含其他信息，只需要简单地完成建立数据链路层连接的工作就可以了。而 LAPDm 协议的这两个帧就没这么好运气了，它们都得干活！为什么 GSM 的 SABM 帧就非得包含信息呢，因为 RACH 信道只有 8bit 的有效信息，我们是根据 3bit 的接入原因和 5bit 的随机鉴别符来区别不同的移动台，但是不幸的是，在高负载的时候完全可能出现两个 MS 的“信道申请”消息中这 8bit 完全相同的情况，而 BSS 系统只会让其中一个接入系统，那么让哪个 MS 接入系统呢？

MS 在调整到相应 SDCCH 信道上要做的第一件事就是给 BTS 发送一个 SABM 帧，该帧包含了详细的接入原因、移动台识别码、移动台类别、传输功率等级、加密算法等。活是挺多的，也实属无奈，谁让 RACH 接入信息就 8 个有用的比特呢，这下只好 SDCCH 信道来还债了。BTS 收到 SABM 帧之后，就不加修改地向 MS 发送一个内容完全一样的 UA 帧，MS 通过将它和本身发送的 SABM 帧进行比较，只有完全一样，才会继续接入，否则它就放弃这个信道，并重新去进行立即指配程序。

BTS 在发送 UA 帧给 MS 的同时，也在 Abis 接口向 BSC 发送一个"建立指示"（Establish Indication）的消息，用于通知 BSC 说 LAPDm 连接已经建立，这算是对立即指配消息的应答。BSC 收到建立指示消息以后，就要求和 MSC 建立 SCCP 连接，以便更有效地交换信息。

上面的内容挺多的，我们来简单地概括一下。因为无线资源稀缺，所以手机进行呼叫或者交换其他信息之前必须首先用"信道申请"命令申请资源。BSC 收到申请信息后，就对资源进行查询和激活，看看是否能满足要求，能满足要求的话就通过"立即指配"命令来让手机接入网络。不幸的是，由于"信道申请"命令所能携带的信息量实在有限，在负载高的时候不足以区分不同的手机，因此在建立数据链路层连接的时候，手机和 BTS 会通过"SABM"帧和"UA"帧的一来一回来判定到底是哪台手机可以接入系统。链路完全建立后，BTS 会向 BSC 发送一条"建立指示"通知 BSC 空中接口的链路已经建立好了，让它心中有数。BSC 此时通常会向 MSC 要求建立 SCCP 连接，准备在 A 接口进行大量数据交换。

随机接入的流程如图 8.15 所示。

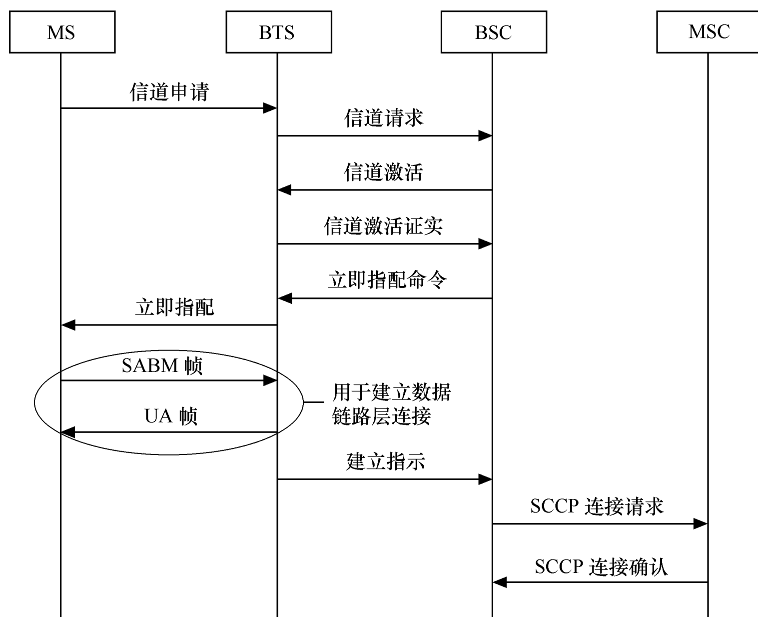


图 8.15　随机接入与立即指配

8.5 你是谁——鉴权的用途及算法

在本节和下节中，我们要关注的是通信的安全。我们不希望被窃听，所以在空中传



递的信号需要加密。但加密之前，我们首先得问一句，你是谁？因为只有知道对方是谁，通信加密才有意义。加密的目的无非是保护双方或对方的通信，如果连对方是谁都搞不清楚，加密就没有任何意义了，因为任何一个闯进来的非法用户都可能访问该信息。所以说，鉴权是任何加密方案的第一步，没有鉴权的加密没有任何意义。

然而，我们所头痛的是，怎样进行鉴权才足够安全，让企图非法闯入系统的人无机可乘？

我们在日常生活中采用的比较多的一个方式是采用用户名和密码来对一个用户进行鉴别，比如说电子邮箱就是如此，输入用户名和密码你就可以进入系统，我们希望把这种方式也应用到 GSM 里面。我们知道，GSM 里有一个标识是可以唯一识别一张 SIM 卡的，那就是 IMSI 号，那就不妨把它当作用户名，再搞一个 Ki 号当密码，我们看看光靠它们两个能不能完成一次安全的鉴权工作。（为了简便起见，假设 IMSI 号为 46001，密码 Ki 为 1234，如图 8.16 所示。）

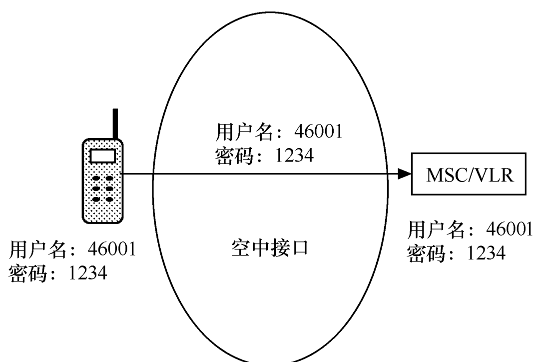


图 8.16　鉴权设想方案 1

我们借用邮箱的方式，用户自己和服务器都各自存储了用户名和密码。手机把用户名和密码通过空中接口发送给 MSC/VLR，然后MSC/VLR和自己数据库的一核对，噢，完全吻合，通过了，你是合法用户。上述过程看上去很美，实际上很不安全，为什么？你的用户名和密码都是明码方式在空中传输，空中的电磁波谁都能接收到，岂不很容易就被人家窃取了，不可行，完全不可行。

有些同学一拍大腿，这密码明文在空中传输，你直接就抄过去了，岂不显得我很傻很天真。不行，我得把密码变一变，于是，他发明了一套 A3 算法，还秘而不宣，除了发送端和接收端，谁也不知道，看你们能拿我怎地。他对鉴权方案 1 稍加改进，效果如图 8.17 所示。

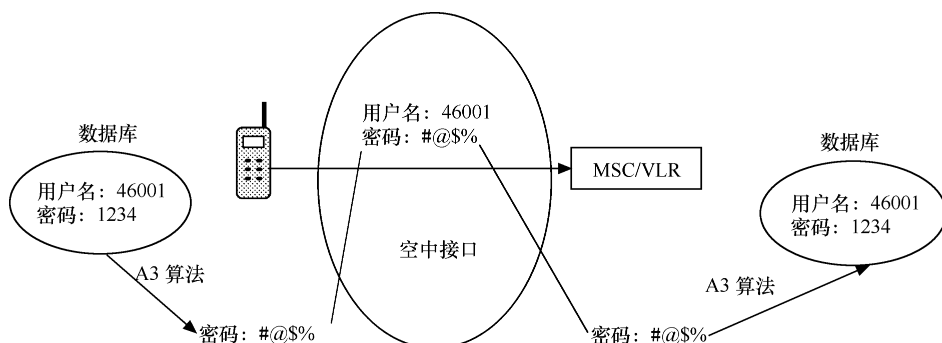


图 8.17　鉴权设想方案 2

这下空中接口传递的不是明文了，好像安全了不少，可以舒舒服服睡大觉了，是这样么？对不起，做入侵的人根本不需要去解密你的 A3 算法，他只需要在空中接口守株待兔，照抄你那一串经过 A3 算法得出的莫名其妙的密文就可以了，我就用用户名 46001，密码#@$%去欺骗服务器，你能怎么地，我摇身一变还是合法用户。

痛定思痛，我们决定在密码的使用上增加一点随机性，让这种单次简单地复制彻底失效。怎么说呢，就是要让空中接口每次传递的用于鉴权的校验密码都不相同，这种简单的重放攻击（replay attack）就无效了！新的设想方案如图 8.18 所示。

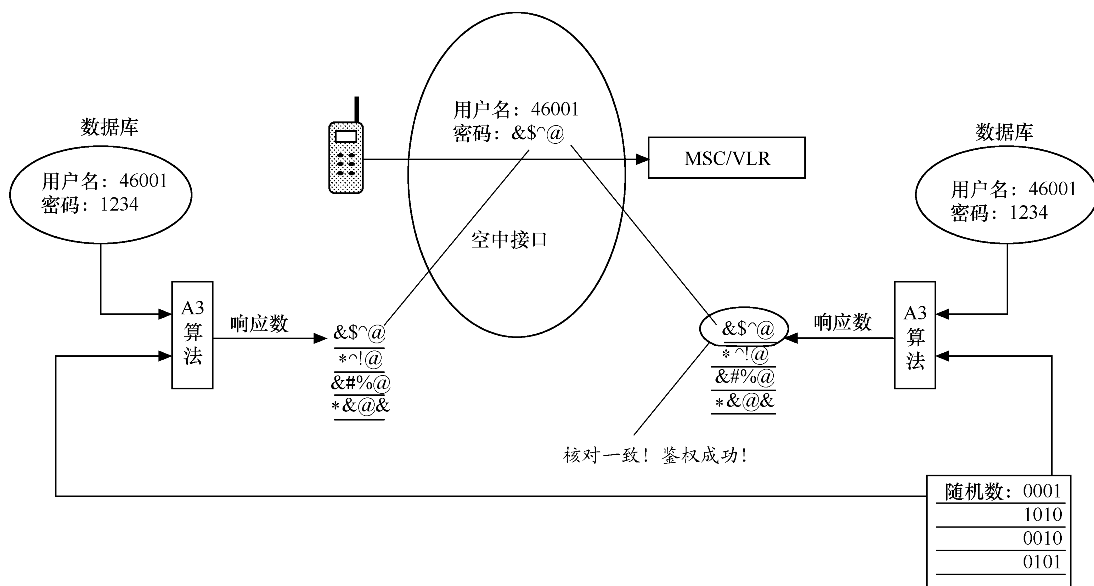


图 8.18　鉴权设想方案 3

这个鉴权设想方案 3 就跟 GSM 里实际的鉴权很类似了，MSC/VLR 的数据库下发一个随机数给手机，两边同时用随机数和密码经过 A3 算法得出一个响应数。如手机算出的响应数和系统算出的响应数一致，那么就可以判定鉴权成功，用户为合法用户。我们可以看到，这个鉴权方案的核心就在于随机数每次都在变化，从而导致响应数每次也都在变化。图 8.18 所示的随机数只有 4 组，这仅仅是示例而已，在真正的网络应用中，这显然不够，只要入侵者足够耐心，窃听 4 次“随机数—响应数”就可以破解了。在真正的无线通信网中，是不会给对手留有这样的机会的，比如 GSM 网中，随机数 RAND 有 128 位，可以表征 2^{128} 个数字，你还指望一组一组地收集数据么？除了随机数的位数要足够多以外，另一个关键的因素是密钥（Ki 值）或者 A3 算法不能公开，一旦公开了，那这个鉴权也就成了摆设，任谁都可以复制这个过程。实际上，在 GSM 网络中，无论是 SIM 卡的 Ki 密钥还是 A3 算法，都是不公开的，是商业机密。图 8.19 就是 GSM 网的鉴权方案。



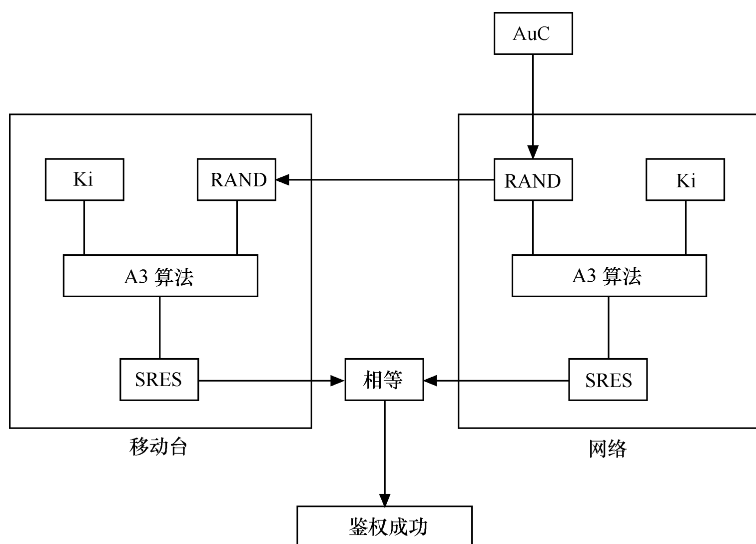


图 8.19　GSM 网鉴权方案

我们知道，鉴权只是加密的第一步，我们在鉴权的时候就要考虑下一步加密的需求。现在密钥 Ki 是存储于 SIM 卡中和网络侧的 AuC 中，鉴权的时候是在 VLR 里对 SRES 进行比对，AuC 可以把 SRES 传给 VLR，反正是一次性的，没什么问题。加密的时候就不同了，加密需要密钥，而网络侧的加密是在 BTS 上完成的，如果拿 Ki 做密钥，那么 AuC 就得把 Ki 传给 BTS，这样很不合适，Ki 毕竟是很核心很机密的数据，不适合明码在网络里传来传去，我们希望能另外弄一个密钥，最好和 SRES 一样，是一次性的。

GSM 的设计者早就对这个问题作了考虑，SRES 不是一次性的吗，那我们就如法炮制一个好了。RAND 和 Ki 经过 A3 算法得出 SRES，我们再搞个 A8 算法，让 RAND 和 Ki 经过 A8 算法得出一个加密用的密钥 Kc，因为 RAND 是随机的，那么 Kc 也就是随机的，这次用的和下次用的不一样，这比直接拿 Ki 出来做加密安全多了。

AuC 通过 A3 算法和 A8 算法就得出了 SRES 和 Kc，那么 RAND、SRES 和 Kc 就一起组成了一个三参数组。一般情况下 AuC 一次产生 5 组三参数组传给 HLR。HLR 可存储 10 组每个用户的三参数组。当 MSC/VLR 向 HLR 请求传送三参数组时，HLR 又一次性地向 MSC/VLR 传送 5 组三参数组。MSC/VLR 一组一组使用，当剩到两组时，就会再要求 HLR 传递三参数组。

了解了鉴权的原理，下面我们来关注鉴权的信令流程，如图 8.20 所示。

当 MS 请求一个业务时（呼叫建立、位置更新、补充业务），VLR 就会触发一个鉴

权过程 VLR 将 RAND 发给 MS，MS 根据 A3 算法得出 SRES，通过鉴权响应命令送给 MSC/VLR，如果核对一致，那么鉴权就通过了。

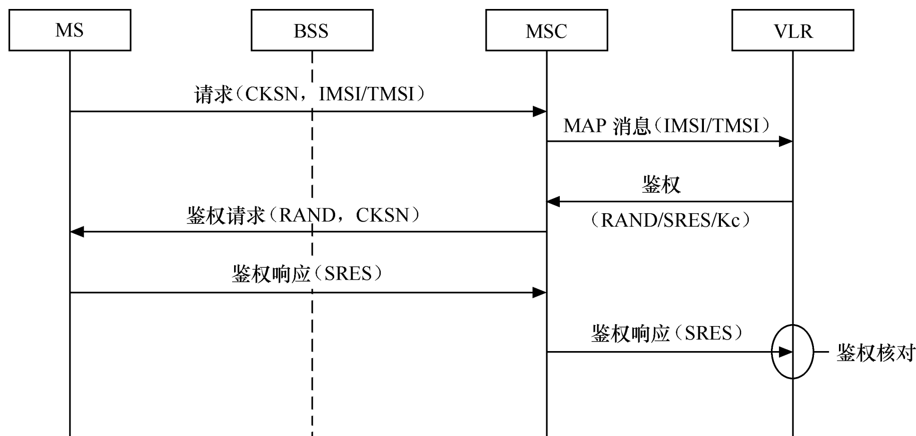


图 8.20　鉴权信令流程图

8.6 加密

加密总是紧跟在鉴权之后，无线通信的加密并不是在所有的通路上，而是仅仅发生在空中接口这个环节。从 BTS 直至 MSC，都是采用明码传输的，因为只有空中接口这一环节是通过电磁波传送的，而电磁波四散传播的特性使得空中接口成为了最脆弱的一环。

8.6.1　加密原理与流程

我们不希望在空中传递的信息被人窃听，那就需要对信息进行加密。然而怎样才能实现加密呢？

首先来考虑邮局的例子，如图 8.21 所示，假设 A 和 B 相隔很远，但是 A 需要向 B 发送一封内容很机密的信件，怎样才能保证信件在运输途中不被人拆开，内容不被泄露呢？

一个通用的做法称为对称密钥加密法（Symmetric Key Cryptography），发送方和接收方拥有相同的密钥，发送方用该密钥对信件进行加密，接收方用该密钥对信件进行解密，如图 8.22 所示。由于只有发送方和接收方拥有密钥，入侵方在中间即使截取了信件，也无法读取信件的内容。



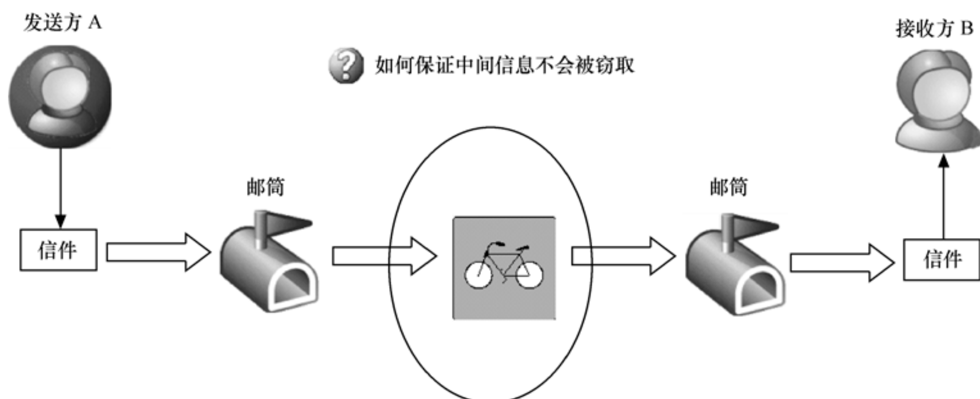


图 8.21　如何保证信息不被窃取

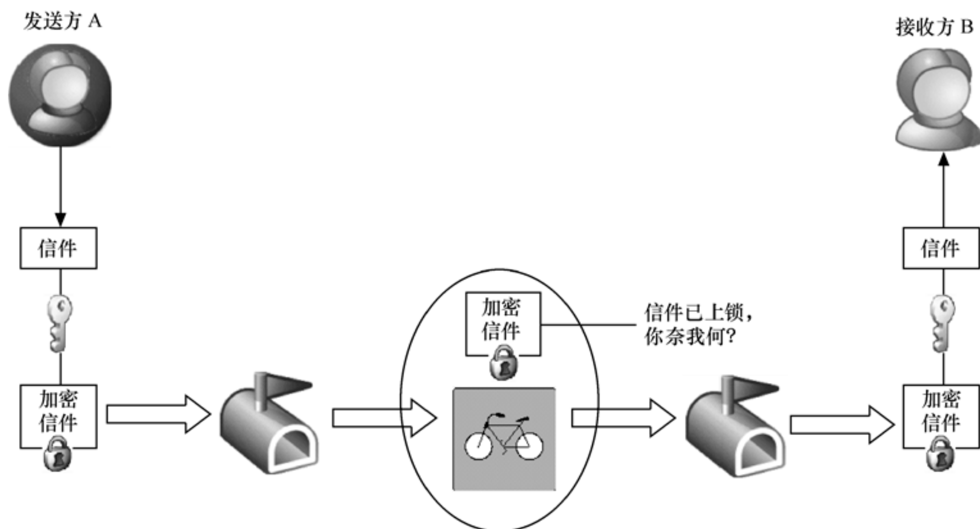


图 8.22　对称密钥加密法

上述理论看起来很美妙，不过我们还是要回到非常实际的问题，那就是无线通信的信号怎样进行加密，或者说一串比特流如何进行加密？将明文变成密文，一种通常的做法就是流加密法（stream ciphers），什么是流加密法呢？

假设字母 a 的 ASCII 码为“01011100”，假设密钥为二进制“10010101”，再假设我们的加密算法为异或，那么加密过程的演示如图 8.23 所示。

文本格式	二进制格式	
a	01011100	明文
	10010101	与密钥进行异或运算
@	11001001	密文

图 8.23　流比特加密法

流加密法又被克劳德・香农称之为混淆（confusion），混淆的目的是保证密文中不会反映出明文线索。实际上，GSM 里面



采用的正是流加密法。问题是密钥该从何而来呢，我们之前说过，IMSI、Ki、RAND 经过 A8 算法可以产生 Kc，Kc 就是用来加密的。一次鉴权产生一次 Kc，由于每次鉴权的 RAND 值都不同，所以产生的 Kc 值也不会相同，按道理用来做密钥进行加密是足够了，但是 GSM 的设计者并不满意，他们打算把这个过程搞得千变万化，复杂无比，让任何企图破译的人都望而生畏。

他们是怎样生成加密的密钥的，他们采用的 TDMA 帧号（22bit）和 Kc（64bit）一起通过 A5 算法来得出加密序列（114bit）！这很要命，Kc 值是每次鉴权产生一个，相对而言时间比较长，TDMA 帧号可是 4.615ms 就变化一次，也就是说每 4.615ms 就变换一次加密序列，要破解可真不容易！

A5 算法及加密过程如图 8.24 所示。

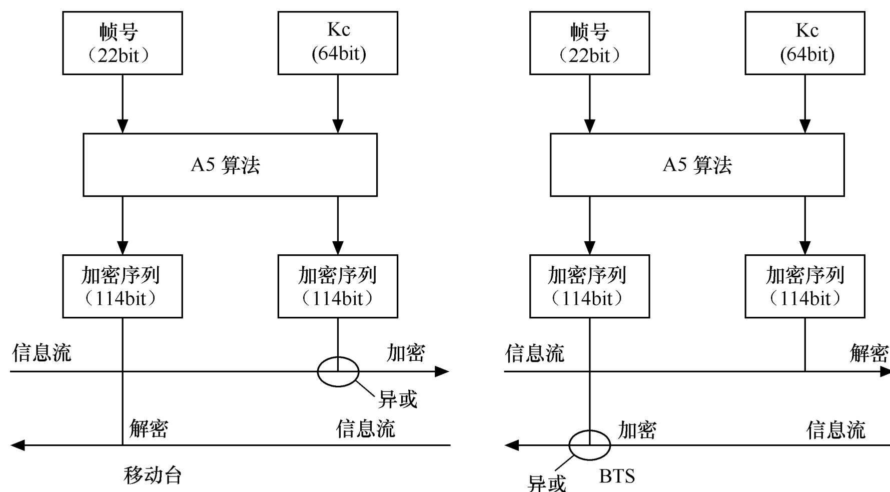


图 8.24　A5 算法

我们看到，整个加密过程 TDMA 帧号是已知的，但 Kc 号和 A5 算法是未知的，只要没有破译 A5 算法和 Kc 号，那么加密就是安全可靠的。

讨论完了加密的原理，我们接下来看看加密的信令流程。

当鉴权过程结束后，MSC 将向 BSC 发向一条“加密模式命令”（Cipehering Mode Command），这个命令是通过 BSSMAP 消息下发的，属于 RR 管理的内容，我们之前说过，BSSMAP 消息就是 RRM 消息在 A 接口的映射。

BSC 接着在信令链路上向 MS 发送“加密模式命令”（Cipehering Mode Command）。MS 收到加密模式命令之后，启动加密模式，然后向网络发送“加密模式完成”消息作为响应。当网络收到“加密模式完成”（Cipehering Mode Complete）消息后，网络将启动在加密模式下的传送，如图 8.25 所示。



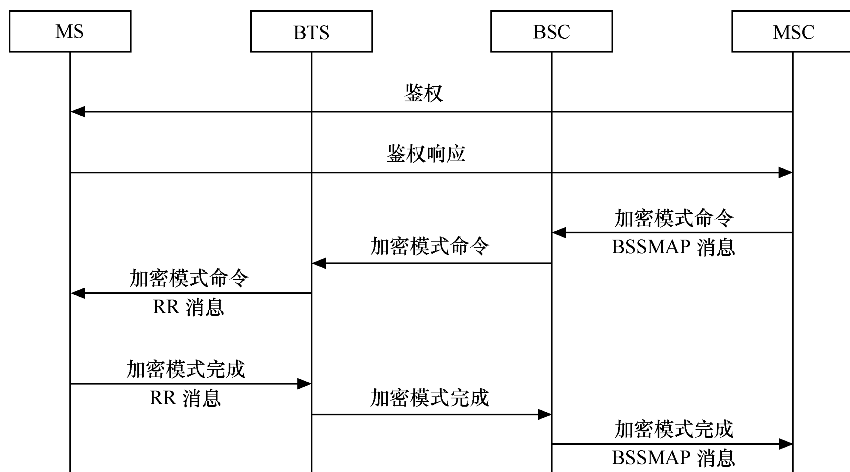


图 8.25　鉴权加密程序

应当注意的是，加密都是紧跟在鉴权之后的，有加密必有鉴权。在图 8.25 中，我们只把鉴权一笔带过，鉴权的详细流程请参见图 8.20。

8.6.2　代号“海狼行动”——TMSI 再分配

有机密的地方就有代号，为的是保密，不让外人知道。在谍战这个需要高度保密的领域，采用代号来代指人或者计划是很普遍的事情，比如央视热播的谍战连续剧《海狼行动》中，行动小组就以“海狼行动”来命名一次夺回国宝龙泉宝剑的计划。

GSM 也是如此，IMSI 号算是比较机密的东西了，它可以用来唯一识别一个用户，就如同你的银行卡号一样，你自然不希望这么一个号码老是在电磁波里传送来传送去了。那么我们就希望用另一个号码来代替它在空中接口传送，也就是代号了，这个代号称为 TMSI（Temporary Mobile Subscriber Identity，临时移动用户识别码）。

TMSI 是 VLR 分配给进入其覆盖区的移动用户的临时识别码。它总是和加密一起使用。TMSI 对每个用户而言是唯一的，因此在呼叫建立、位置更新等过程中，可替代 IMSI 在空中接口上使用，另外，TMSI 可根据网络需要，每次或若干次空中接口操作后（如呼叫建立、位置更新），重新分配一次，因此能有效地保护用户在无线通道上不被识别。一般而言，若位置区改变以及鉴权加密之后，是应该重新分配 TMSI 的。

首先我们来看看位置更新，当移动台在位置区内第一次注册时，就会将一个 TMSI 分配给移动台，当移动台离开该位置区时就会释放该 TMSI 号码。MS 收到 TMSI 的再分配命令之后，将把所收到的 TMSI 和 LAI 存储在 SIM 卡内，并向网络发送“TMSI 再分配完成”的消息。

无论当前的 TMSI 是否能被系统识别，出于对用户身份保密的考虑，在每次通信时，

网络都可以为 MS 重新分配一个 TMSI。TMSI 的再分配程序一般是在加密完成之后，SETUP 建立之前，这是为了对 TMSI 进行加密从而实现保密的作用。

TMSI 分配的信令流程图如图 8.26 所示。

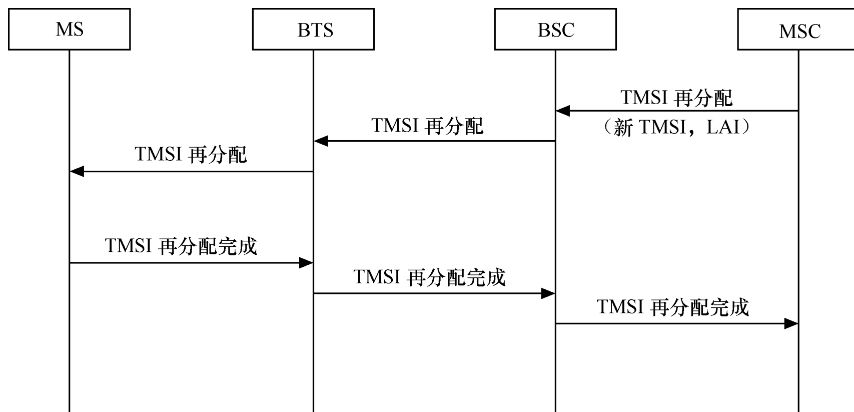


图 8.26　TMSI 再分配流程

8.7 记得给妈妈打电话报平安——位置更新与IMSI附着

位置更新其实属于 MS 空闲状态时的内容（参见 8.2 节），我们之所以把它放到后面是因为位置更新属于 MM 连接的内容。MM 连接必须建立在 RR 连接之上，没有随机接入就没有位置更新。因此把位置更新放在了随机接入之后。

我们在 1.3.3 节中就提过，这位置更新就跟家里报平安没什么两样。你在外面晃悠，家里希望有事的时候能够找到你，所以你最好到了一个新的地方就给家里打电话，这叫“正常位置更新”；就算地方没动，隔段时间也要给家里打电话，免得家里担忧，这叫“周期性位置更新”。

位置区是随着蜂窝通信的发展而产生的，在模拟通信时代是没有什么位置区的概念，一个 MSC 包打天下。如果要寻找一台“大哥大”，那么就在该 MSC 下所有的基站下发寻呼消息寻找该手机好了。随着蜂窝通信的飞速发展，原先的方式渐渐不行了，手机用户越来越多，如果寻找某台手机就要在 MSC 全区下发寻呼消息，这个系统负荷也太大了。于是就引进了“位置区”（Location Area）的概念，划分出位置区之后，我们就可以分片对手机进行寻呼，或者说按位置区对手机进行寻呼。

MSC 下的网络被划分为若干个位置区，一个位置区可以包含多个小区。位置区用位置区标识（Location Area Identity，LAI）进行标注，LAI 会在系统消息 3 和系统消息 4



中广播。手机会主动向网络报告自己所在的位置区，而网络会存储每个手机所在的位置区，那么一旦需要寻找该手机，就知道在什么范围内对该手机进行寻呼。

所以说当手机从一个位置区移动到另一个位置区时，它必须进行登记，要不然网络就不知道它所在的位置，没法对它进行寻呼。这就好比寻人启事一样，你总得知道你要找的人的大致区域，才好去相应的区域打寻人启事广告。那么手机如何发现自己到了新的位置区呢？它是通过解码小区广播信道上的系统消息，发现 LAI 发生了变化，从而知道自己到了新的位置区的。

8.7.1　位置区的设置

这位置区的划分是件麻烦事，应当说位置区过大和过小都不太好。位置区过小，那么 MS 的位置更新必然增多，就会增大网络的信令流量；如果位置区过大，那么一个寻呼消息需要下发的小区就会增多，同样会增加寻呼信道的信令负荷。所以说划分位置区实属一门艺术，需要在位置更新和寻呼之间寻找平衡，我们的理想状态应是在保证不会产生寻呼负荷过高的前提之下尽量使位置更新次数降到最低。位置更新是要占用系统资源的，包括无线资源还有有线信道的资源，但又不会带来任何收入，所以说频繁的位置更新对运营商来说是不划算的。

我们在上面说过，当手机从一个位置区移动到另一个位置区时，它必须进行登记。那么当手机处于两个位置区的边界时，就会发现我们遇到了麻烦，那就是不知道该怎么应对小区重选引发的位置更新！

小区重选对于无线通信而言实在是件很平常的事情，因为无线环境是不断变化的，手机一发现信号强度更高的小区就会更换所驻留的小区，以谋求更好的通信质量。本来频繁的小区重选对网络没有什么直接的影响，但是当手机处在位置区的边界，情况就不一样了，它很可能在处于不同位置区的几个小区之间重选来重选去，从而导致频繁的位置更新。虽然我们规定了，由 $C2$ 引起的两个小区重选之间至少要间隔 15s，但是如果过多的手机进行位置更新，这 15s 是没有什么作用的。这势必给网络带来很大的信令负荷。

为了避免在边界处有过多的位置更新，我们首先建议 LA 区域边界的划分最好不要在人口密集、话务量高的地方，而最好选在人烟稀少、话务量较低的地方，从而减少进行位置更新的手机的数量。其次，我们引入了 CRH（Cell Reselection Hyseteresis，小区重选滞后）参数，这个参数的作用就是要求邻小区信号强度必须比服务小区强度高很多（高于小区重选滞后值 CRH），才能启动小区重选。等于说是为小区重选设置一个门槛障碍，不是比当前小区好太多就不要进行重选了，以免进行频繁的位置更新浪费网络资源。

8.7.2 位置更新信令流程

MS 的位置更新分为 3 类。

（1）MS 来到一个新的位置区，发现小区广播的 LAI 与自身不一致，从而触发位置更新。系统需要对 MS 进行寻呼，那么就必须知道 MS 当前的位置区，所以说这个过程就是必需的，也称为“正常位置更新”。

（2）由参数 T3212 定义的周期性位置更新。为什么要设置这个参数呢？周期性的位置更新是因为有时候 MS 进入了信号盲区或者突然掉电，如果这时候还对 MS 进行寻呼显然是浪费资源。那么我们就要求 MS 周期性地上报自己的位置，凡是没有进行周期性位置更新的 MS，我们就给它贴一个“分离”的标签，不再对这样的 MS 进行寻呼。实际上，这就是一种处理 MS 非正常脱离网络的手段。

（3）IMSI 的 Attach 和 Detach。当 MS 关机时，会给系统发送一条“IMSI Detach”指令，告诉系统该 MS 已经脱离网络了，不要再对其进行寻呼，网络就给 MS 贴上“分离”的标签。当 MS 开机时，会给系统发送一条“IMSI Attach”指令，告诉系统 MS 可以重新被寻呼了，网络给 MS 贴上“附着”的标签。如果开机的时候发现当前所处的位置区与 MS 的 SIM 卡存储的位置区标识不一致，还会触发位置更新，在系统里更新自己的位置区。

讨论完了基本的概念，下面来关注一下实际的信令流程。

1. 正常位置更新

所谓“正常位置更新”就是发现 LAI 发生变化时 MS 主动申请进行的位置更新。如果手机正在通话，又发现从 SACCH 信道发送的系统消息 5 和系统消息 6 中的 LAI 与 MS 里存储的不一致，那么就等通话结束后进行位置更新。

MS 经 SDCCH 信道向系统发送位置更新消息，根据这次位置变化后是否还在同一个 MSC/VLR 里把正常位置更新分为两种情况，这两种情况的信令流程有所不同：一种是新 LAI 与原 LAI 同属一个 MSC/VLR，此时只要 MSC 简单地修改一下 MS 的位置信息即可；另一种是跨 MSC 的位置更新，这就要复杂很多，因为新的 MSC 并没有当前 MS 的数据。此时新的 MSC/VLR 就向 HLR 发起位置更新请求，HLR 接收并修改 MS 所在的 MSC 信息（MSCID），并通知原来的 MSC/VLR 删除该 MS 的相关信息。原来的 MSC/VLR 删除相关信息之后，向 HLR 发回“删除位置确认”消息。此时在新的 MSC/VLR 区域需要完成鉴权加密以及 TMSI 再分配的过程，当此过程完成之后 HLR 将会向 MS 当前所在的 MSC/VLR 发送一条“插入用户数据”的信息，将向该 VLR 提供它所需的用户信息，当 HLR 收到 VLR 的响应时就向该 VLR 发出位置更新确认的消息。



上面这段话怎么理解呢？同一个 MSC/VLR 内的位置更新相当于公司内部调动，你只需要在公司人力资源部备个案（在 MSC/VLR 里登记），注明当前所在的部门（位置区）就行了；不同 MSC/VLR 的位置更新相当于跳槽到另一个公司，那么流程自然要复杂很多，新的公司没有你的档案，就向当地劳动局（HLR）提出更改这个职员所在的公司信息（在 HLR 里修改当前 MS 所在的 MSCID），劳动局（HLR）是存储了这个职员的档案的（HLR 里当然存储了 MS 的用户信息），它先要求职员原先所在的公司删除相关档案（前 MSC/VLR 删除用户数据），然后给新的公司发送该职员的档案。

（1）相同 MSC/VLR 的位置更新流程如图 8.27 所示。

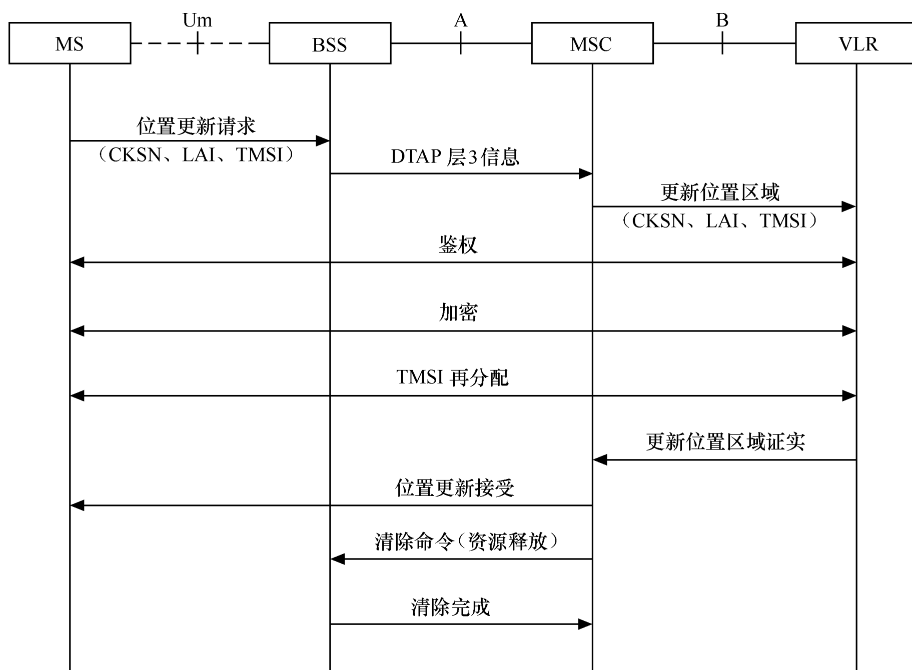


图 8.27　相同 VLR 位置更新流程

（2）不同 VLR 的位置更新。

如果 MS 进入了另一个 VLR，那么 MS 在 HLR 里的 MSC 地址（MSCID）也需要进行改变，因此此时的位置更新必须涉及 HLR。

具体流程如下：MS 从一个 BTS 小区移向不同的 MSC 的另一个 BTS 小区时，由于 MSC 地址发生变化，所以新的 MSC/VLR 向 HLR 发出位置更新请求，给出新的 MSC 和 MS 的识别码（MSCID&IMSI/TMSI）。HLR 修改该用户数据后，回给 MSC 一个响应，VLR 对该客户进行注册并从 HLR 下载相关数据，同时 HLR 通知原来的 MSC 删除 VLR 中有关该 MS 的客户数据。不同 VLR 位置更新的信令流程如图 8.28 所示。

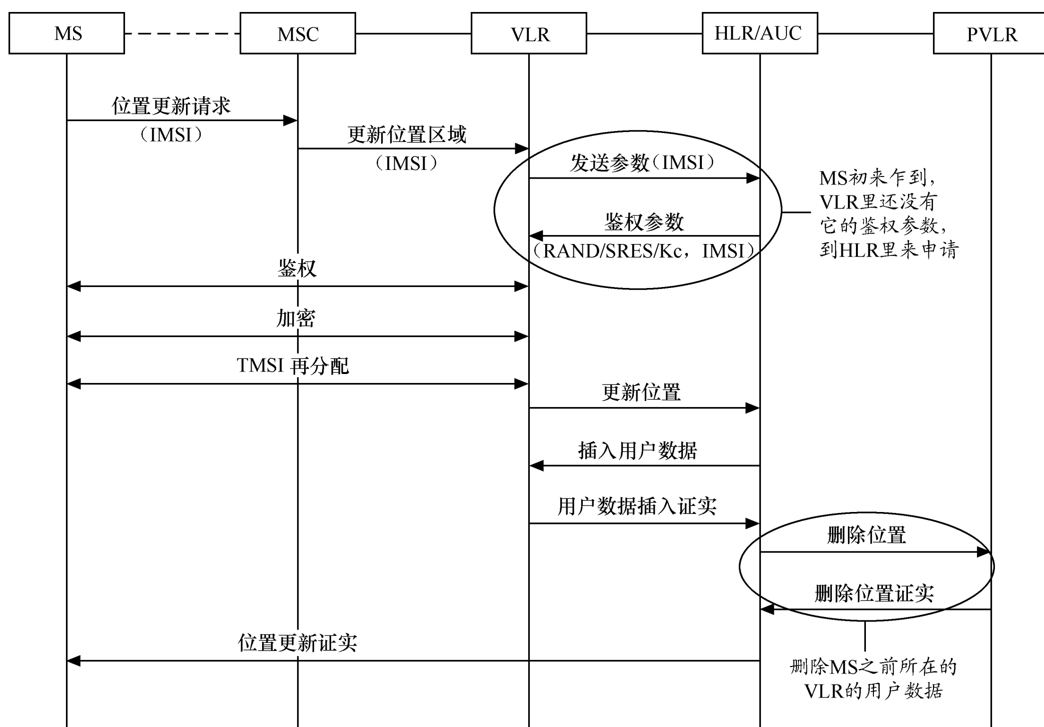


图 8.28　不同 VLR 位置更新流程

2. IMSI Attach/Detach

首先问个问题，按键关手机和直接拔电板有何不同？一般人或许不会认为有什么不同，不都是通过断电让手机关机嘛。其实是大有不同的，按键关机的话手机会向网络送一条指令，指示网络自己关机了，而直接拔电板就没法发送这条指令了。所以大家可以试试，关机的话用别人的电话拨打你的手机得到的应答是：“您拨打的电话已关机”，说明网络已经知道你关机了；而拔电板的话得到的提示是：“您拨打的电话不在服务区，请稍候再拨”，这时候网络并不知道你的手机已经关机了，于是就在网络下发 Paging 消息来寻找你，但是找不到，于是就默认为你“不在服务区”了。

手机开机和关机的信息对网络而言很重要，因为你开机，别人就可以去找到你，你关机，别人就没法找到你，所以手机的开关机信息是一定要告诉网络的。我们都知道，MS 用户在网络里是用 IMSI 来识别的，那么这个开关机信息就称为“IMSI Attach/Detach”。

当 MS 开机接入网络后，便“附着”在网络上，随时可以和网络进行信令的交互，如果需要寻找该 MS 时，只要看到该 MS 是“附着”状态，就可以根据它的位置区信息对其进行寻呼。当 MS 正常关机时，将向网络发送最后一条消息，即分离消息，其中包



括分离处理请求，当 MSC/VLR 收到该消息后，在该 MS 对应的 IMSI 上作“分离”标记，此后网络看到该标识就不需要再发送寻找该移动用户的寻呼消息，免得浪费网络资源。

分离程序只在 MSC/VLR 里进行，HLR 并不会得到任何通知。这个做法也有利有弊，好处在于，不必每次开关机都通知 HLR，节省了“HLR-VLR”这一段路由资源；不利的地方在于，每次对“分离”用户进行呼叫时，HLR 还需要去 MSC/VLR 里查询该用户的当前状态，从而浪费了“HLR-VLR”这一段路由资源。权衡利弊，GSM 规范还是决定“IMSI Attach/Detach”消息到 VLR 为止，不通知 HLR。

下面我们来详细介绍“IMSI Attach/Detach”的信令流程。

（1）IMSI Attach 流程

若 MS 开机后发现它所存储的 LAI 号与当前所在位置区的 LAI 号一致，那么它就不进行位置更新，而仅仅进行 IMSI 附着过程。IMSI 的附着过程与 VLR 内部的位置更新过程基本一致。唯一不同的是，这里位置更新申请注明的原因是 IMSI 附着。IMSI 附着的信令流程如图 8.29 所示，为了简便起见，我们在流程图上略去了鉴权、加密和 TMSI 再分配的过程。

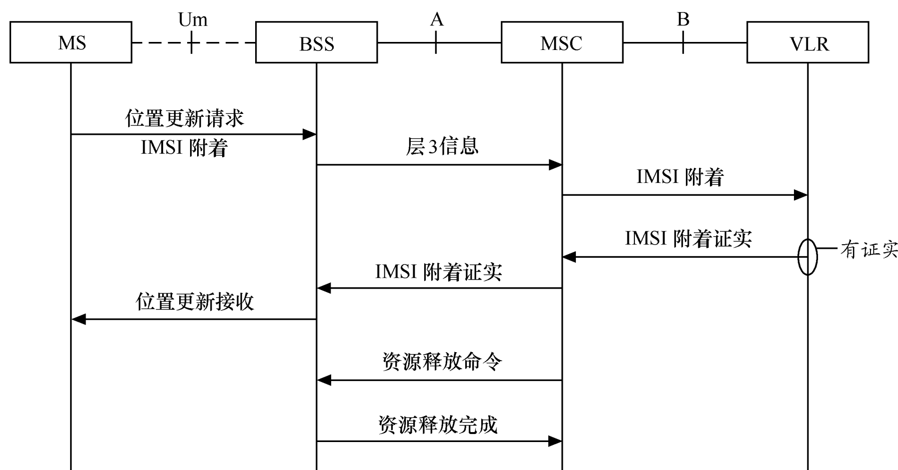


图 8.29　IMSI Attach 流程

（2）IMSI Detach 流程

当 MS 切断电源关机时，MS 即向网络发送最后一条消息，其中包括分离处理请求，MSC 收到后，即通知 VLR 对该 MS 对应的 IMSI 作“分离”标记，而归属位置寄存器（HLR）并没有得到该客户已脱离网络的消息。当该客户被寻呼时，HLR 要向拜访的 MSC/VLR 要漫游号码（MSRN）时，MSC/VLR 通知 HLR 该客户已经脱离网络，不再需要发送寻找该客户的寻呼消息。网络随即向主叫返回一条“您拨打的用户已关机”的应答。

IMSI Detach 的信令流程如图 8.30 所示。从图中可以看出，IMSI Detach 与 IMSI Attach

是有着很大的不同的。IMSI Attach 信令是一条证实信令，有收有发；而 IMSI Detach 是一条无证实的信令，网络收到该消息后不需要给 MS 发送证实消息，因为 MS 已经关机了。如果 IMSI Detach 消息出现故障，那么 MS 也是无法重发消息的，原因同上。

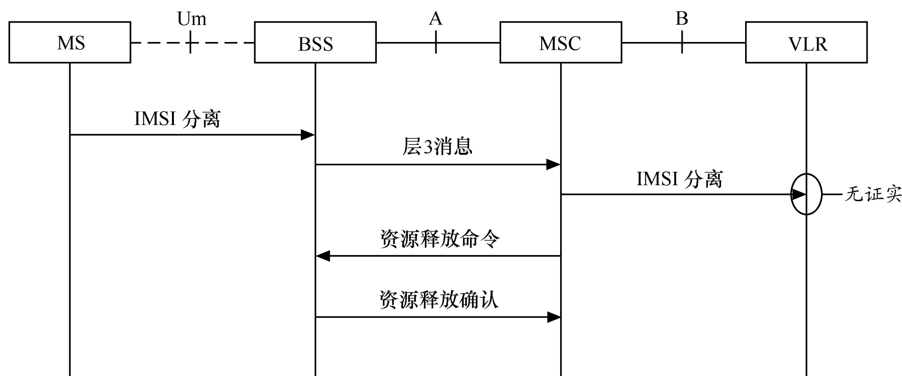


图 8.30　IMSI Detach 流程

3．周期性更新

我们试想一下，MS 由有信号的区域走向无信号的区域，突然拔掉 MS 的电板，甚至是 MS 关机时发送的“IMSI Detach”消息，都会使得网络对 MS 依旧标注“附着”状态而实际不可达。一旦拨打该 MS 时，网络将试图寻呼该 MS，而实际上此时该 MS 已经无法接听电话，这就会使系统不断下发寻呼消息，占用无线资源，从而使得寻呼成功率和接通率有所下降。

为了解决这个问题，GSM 系统采取了相应的措施要求 MS 在经过一定的时间之后，自动向网络报告当前的位置信息。若超过规定的时间依然没有收到 MS 发送的周期性登记信息，那么系统将认为该 MS 已经关机或不在服务区，然后在 MSC/VLR 里将该 MS 标注为“分离”。仅当网络再次收到 MS 的位置更新信息或“IMSI 附着”信息时，才再将 MS 改为“附着”状态。

这个规定的周期更新的时间间隔称为“T3212 参数”，该参数在系统消息 3 的“控制信道描述”中下发。MS 收听 BCCH 载频上系统消息 3 上广播的周期性位置更新的时间。MS 自身有关于位置信息的计数器，每当 MS 从专用模式返回空闲模式时，该计数器复位，开始计时估算自己多长时间之后需要向网络汇报自己的位置信息。

设想一个问题，假设现在规定的 T3212 时间是半小时，现在系统对这个参数进行了修改，变为了一小时，那么怎么办，是不是该小区所有的 MS 的计数器都复位归 0，然后一小时之后同时进行位置更新？

这显然是一种很糟糕的假设，我们希望 MS 位置更新的时间尽量错开，免得大家



一起争抢无线信道。这跟银行有点类似，银行也不希望客户都在同一时间去取钱，那叫“挤兑”。

为了避免这种糟糕的情况，我们需要在 MS 计数器的设置上动一点脑筋。如果 MS 收听到系统广播中的 T3212 的值改变时，该计时器就将重新计时，该计时器的数值改为：“当前剩余值”MOD“新的 T3212 值”，如果新的 T3212 值比原来的要大，那么 MS 就保持当前的计时器剩余值。这是什么意思呢，我们举个例子来看看。

假设 MS 当前的计时器的值为 0.6h，若新的 T3212 的值为 0.5h，那么计时器的值将改变为 0.6mod0.5=0.1h；如果新的 T3212 比现在计时器的数值要大，假设为 0.8h，那么新的计时器的数值不会发生变化 0.6mod0.8=0.6h。和一个比自身大的数值进行求余运算其结果等于本身。这个措施可以保证 T3212 的值发生改变后，每个 MS 的计时器的指示值都不尽相同，从而避免了网络中所有的 MS 在同一时间内进行周期性位置更新，不至于使网络在某一时间遭遇高负荷。

周期性位置更新的时间参数 T3212 到底设为多大也有讲究。我们可以很明显地知道，这个数值设置过大肯定是不利的，这会导致网络不能及时地更新 MS 的状态，从而会有很多的无效寻呼，降低了寻呼成功率。如果这个参数设置过小带来的好处是我们可以及时掌握 MS 的动态，但同时也会有负面的影响，那就是会使网络的信令流量的负荷大大增加并使手机的待机时间缩短。所以我们需要求一个合适的 T3212 参数来兼顾两者的平衡。

8.8 让我们来搭积木——MS主叫流程分析

到了主叫和被叫的信令流程分析这一阶段，就跟搭积木似的：前面的随即接入、鉴权与加密、TMSI 再分配一股脑地涌了过来，再加上对 TCH 信道的分配，就成了主叫的信令流程。被叫的信令流程需要在此基础上再添加从 HLR 去取被叫路由以及对被叫进行寻呼的过程。被叫相对主叫而言之所以会更麻烦，是因为被叫用户所在位置的不确定，我们需要通过寻址和寻呼来建立至被叫 MS 的路由。之所以在学习主叫和被叫流程之前，还建议大家对之前的内容进行一下复习，夯实一下基础，是因为主被叫信令流程很大一块内容是前面内容的堆砌。

MS 用户做主叫也称为 MO（Mobile Originate），其信令过程是从 MS 向 BTS 请求信道开始的，到主叫用户 TCH 指配完成为止。一般而言就是分为以下几个阶段：接入阶段、鉴权加密阶段、TCH 指配阶段。

接入阶段主要包括信道申请、信道请求、信道激活、信道激活证实、立即指配等几



个步骤，经过这几个步骤，手机建立了自 MS 至 MSC 的一条路径通道。无线通信相对有线通信不是缺少一条固定的传输通道吗，那么接入阶段就是为了弥补这个问题。

鉴权加密阶段主要包括鉴权请求、鉴权响应、加密模式命令、加密模式完成、TMSI 再分配等几个步骤。经过这几个步骤，主叫用户的身份得到了确认，网络认为该主叫用户是一个合法用户，允许继续进行呼叫，并对呼叫信号进行加密。我们在第 1 章就说过，无线通信相对有线通信而言，一是用户身份不好确定，二是无线通信的信号是在空中通过电磁波四散发射的，其安全性是很成问题的，所有这一阶段的主要任务还是为了弥补移动网相对固网的缺失，即身份确认和通话安全。

TCH 指配阶段主要包括指配命令、指配完成。经过这个阶段，主叫由 SDCCH 信道转换为 TCH 话音信道。如果在后面的被叫接续过程中没有接通，那么主叫可以通过话音信道听到 MSC 的提示。

在这里，我们将这几个过程完整地再梳理一遍，以便让大家对手机主叫的整个信令流程有一个清晰的认识，也是对前面内容的一个复习。

1. 第一阶段——接入阶段

（1）MS 信道请求

如果一个 MS 处于空闲状态，用户要进行通信，那么只要他属于被叫号码，再按“发送”按钮，MS 便开始启动主叫程序。

我们知道，随即接入的目的就是要建立一条自 MS 至 MSC 的 RR 连接。那么 MS 先通过随即接入信道 RACH 向系统发出的第一条消息就是“信道申请”（Channel Request）消息，要求网络提供一条 SDCCH 信道用于信令的传递。

BTS 收到 MS 的“信道申请”消息后，接着通过 Abis 接口向 BSC 发送一条“信道请求”（Channel Required）的消息，这条消息包含了 BTS 对传输时延（TA 值）的估计，我们知道，GSM 是一个 TDMA 系统，为了避免时隙间相互干扰，对每个 MS 的信号在空中的传输时延的测算就非常重要。

（2）BSC 对信道进行激活

BSC 收到该条信息后，根据对现有系统无线资源的判断，为该次请求选择一条相应的空闲信道给 MS 用。BSC 仅仅是从数据库里挑选出一条信道给 MS 用，该信道是否真的可用，那还得实践才能出真知，于是 BSC 向 BTS 发送一条“信道激活”（Channel Active）消息来查询相应的地面资源（传输电路等）是否可用。BTS 在准备好相应的资源后，将返回一条“信道激活证实”（Channel Active ACK）消息来答复 BSC。

（3）BSC 为 MS 指配信道

信道既然已经激活了，万事俱备，BSC 于是在允许接入信道（AGCH）中通过下发



立即指配（Immediate Assignment）消息通知 MS 为其分配的专用信道。立即指配消息的目的就是为了建立一条自 MS 至 MSC 的 RR 连接。

值得注意的是，并不是所有的“信道申请”消息最终都会被分配信道，若 BSC 发现没有信道分配时，网络将以无证实的方式向 MS 发送“立即指配拒绝”（Immediate Assignment Reject）消息，所谓的无证实的消息就是有来无回的消息，一般情况下的信令都是有来有回的，但是 BSC 俺都说了俺这里资源紧张了，你再发条信息过来浪费资源不是欠扁么。

（4）MS 回送 SABM 帧已确认接入信道

MS 收到立即指配消息后，就转换到指定的 SDCCH 信道上，然后在该信道上发送 SABM 帧（CM 业务接入请求）用于建立数据链路层的连接。

（5）建立 A 口的 SCCP 连接

我们通过立即指配和信道激活指令建立了自“MS-BSC”的链路，要完成一次呼叫，还需要在 A 接口建立链路，以完成“MS-MSC”的完整通道。应当说 BSC 至 MSC 是有链路的，MTP 连接是在通话前就建立好了的，但是我们每次呼叫还需要在 MTP 层之上建立 SCCP 链路。因为 A 口的信令消息都是通过 SCCP 进行传输的，你不能光打电话不传信令啊，所以 SCCP 连接那是必需的。SCCP 连接建立之时 BSC 向 MSC 发送 CM 业务请求信息。

至此我们就建立了自 MS 至 MSC 的完整通道，也就是 MS 至 MSC 的 RR 连接，RR 实体就通知 MM 子层已经由空闲模式进入了专用模式。

2．第二阶段——鉴权加密阶段

（1）鉴权阶段

SCCP 连接建立起来了，MSC/VLR 收到了 MS 发送的 CM 业务请求信息，接下来系统就首先需要对移动台的身份进行鉴定，干活之前我得先验证一下你是不是我的客户啊。VLR 于是向 MSC 下发鉴权指令，MSC 收到后再通过 BSS 系统透明向 MS 下发鉴权请求（鉴权属于 MM 消息，BSS 系统不作处理，直接转发）。MS 收到鉴权请求后，根据鉴权算法得出响应数 SRES 送达 MSC/VLR，VLR 把自己产生的 SRES 和 MS 产生的 SRES 进行比对，如一致则鉴权通过，如不一致则拒绝 MS 的接入请求。

（2）加密阶段

我们在通话过程中有很多敏感信息，而电磁波的特性又如此公开，因而我们希望对信息进行加密。鉴权通过后，VLR 将首先向 MSC 下发加密模式命令，然后下发“接收接入请求”（Accept Access Request）消息，作为对 MS 的“CM 业务请求”的回应。MSC 向 MS 下发“接入请求消息”和“加密模式命令”，MS 收到此命令并完成加密后，回送

“加密模式完成”的消息来响应 MSC 的“加密模式命令”，以向 MSC 表明 MS 已经可以使用安排的密钥进行加密了。至此 MS 就完成了第一阶段和第二阶段的工作。为了方便起见，我们把处于准备阶段的随机接入以及鉴权加密单独画出来，如图 8.31 所示，因为主叫的所有流程都画在一起的话那未免也太长了。

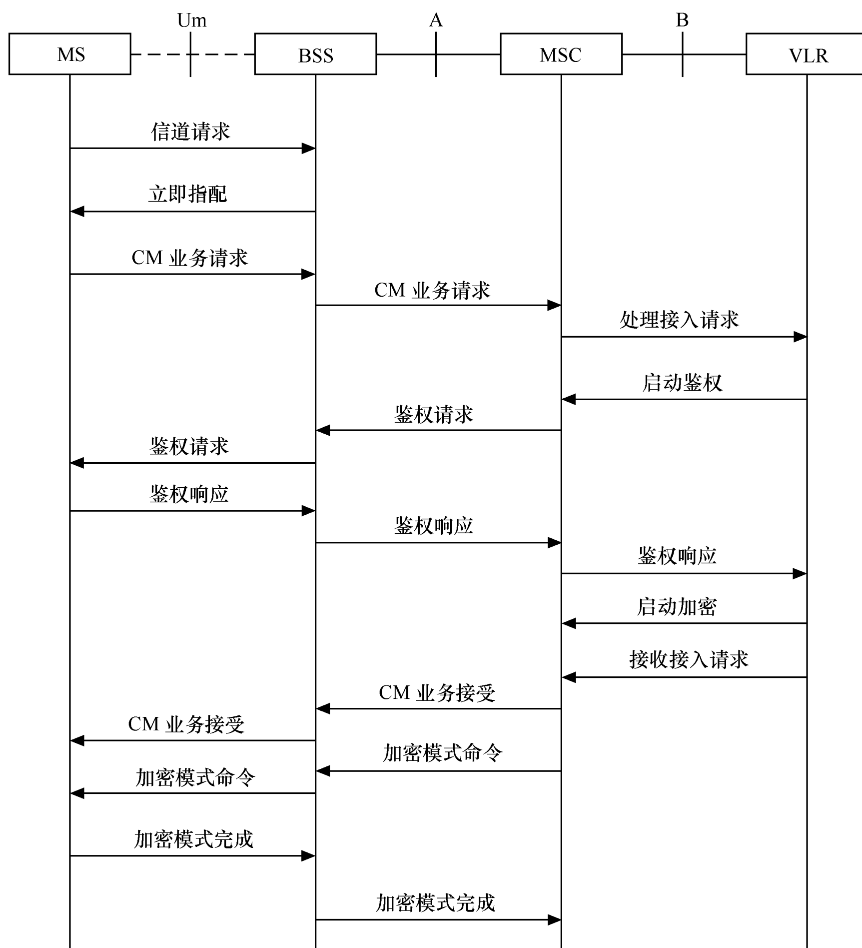


图 8.31　手机主叫之随机接入与鉴权加密

3. 第三阶段——呼叫建立阶段

第一阶段和第二阶段的工作我们在前面的章节里都已经讲过，在这里只当是复习，算是我们搭积木盖房子的地基。移动网相对于固网，首先是没有一条固定的传输路径，这就是第一阶段随机接入需要解决的问题；其次移动网的传播载体电磁波太不安全了，需要鉴权和保密机制来弥补这个缺陷，这是第二阶段需要解决的问题。



下面是本节真正要关注的问题，也就是主叫的第三阶段——呼叫建立阶段。话说路径和安全问题解决好以后，移动通信剩余的主叫接续过程与固网基本一致，这个问题也很容易相通，本来移动网与固网的不同点就是路径与安全这两项，这两个问题解决了，移动网和固网也就大体相当了，对于电信网这么一个注重传承的网络而言，当然是多一事不如少一事，照抄固网的好了。

我们首先来回忆一下固话的主叫过程：首先提起电话拨号，拨号其实向网络送出的不仅仅有号码信息，还包括了业务类型等一系列隐含消息，以便于网络进行处理；拨号完成后我们通常会听到“嘟——嘟——嘟”的回铃音，这个过程通常称为“提醒”（Alerting），也就是提醒被叫摘机的意思；如果被叫摘机了，我们通常会听到一声脆响，就是用户摘机的声音，这个过程称之为“连接”（Connect），这很好理解，被叫摘机了，那么主叫和被叫就自然“连接”了。

我们接下来关注一下无线通信的主叫过程：无线通信第一步也是要拨号，把主叫的相关信息传送给网络；第二步有所不同，为了节省空口无线资源，在接入的初始阶段通常会给 MS 分配 SDCCH 信道，初期的加密鉴权过程需要交互的信息不多，采用 SDCCH 这样的小容量信道很合适，但现在要进入语音通信阶段了，那么就得分配一条 TCH 信道了，这个过程是固网所没有的；接下来的“提醒”（Alerting）与“连接”（Connect）与固网并无二致。

（1）MS 的呼叫类型信息

首先移动台在 SDCCH 信道上向网络发送一个“Setup”消息，用于向 MSC 提供更为详细的消息。消息内容包括：本次呼叫请求的具体业务类型及 MS 能提供的承载能力、被叫用户号码，其中对于补充业务还可以包含各类附加的信息。

（2）话音信道指配过程

当 MSC 收到“Setup”消息后，首先向 VLR 查询该用户的相关业务信息，VLR 根据此次的业务类别和开户时 MS 已经申请的业务信息，决定此次呼叫是否可以继续。这个过程有什么意义呢？因为并不是每个呼叫都是可以继续进行的，比如说拨打国际长途，假如你没开，在这里就直接给拒掉了。

如果 VLR 判断这个呼叫业务不能继续，则向 MS 发送“释放完成”（Release Complete）消息，呼叫建立就此失败，然后再把底层的信令释放掉，转入空闲状态。如可以通过，则 VLR 向 MSC 发回“完成呼叫能力查询”的消息，指示 MSC 可以进行下一步动作。只有呼叫能够继续才会给你分配 TCH 信道，够抠门儿吧！

MSC 收到该消息后，就向 MS 回送“呼叫进程”（Call Proceeding）消息，告诉 MS 呼叫还在继续处理中，让 MS 少安毋躁，继续等待。然后 MSC 根据业务请求的需要向 BSC 发“指配请求”（Assignment Request）消息，要求 BSC 来给此次呼叫分配 TCH 信道。BSC 收到该指令后，如果发现有所需资源的话就会向 BTS 发送一条“信道激活”

（Channel Activation）指令以激活相应的地面资源；等 BTS 将电路资源准备好以后，就会向 BSC 发出“信道激活证实”（Channel Activation ACK）消息。BSC 接着就通过 SDCCH 信道给 MS 发送“信道指配”消息，安排 MS 到指定的空闲信道 TCH 上进行话务接续。TCH 指配及接续过程如图 8.32 所示。

MS
BSS
MSC
VLR
HLR
被叫 MSC/VLR
呼叫建立
呼叫建立
查询用户信息
完成呼叫查询
呼叫进程
呼叫进程
指配请求
指配请求
指配完成
指配完成
路由信息请求
提供漫游号码
回送漫游号码
寻找被叫的过程，本节暂不讨论
回送漫游号码
IAI（IAM）消息
ACM 消息
提醒
应答
连接
连接证实

图 8.32　TCH 指配及接续过程

我们可以看到，话音信道的指配过程和立即指配的过程非常相似。不同点在于立即指配是 BSC 根据“信道请求”消息下发的，触发点在 BSC；而话音信道的指配是由 MSC 触发的。共同点在于都需要 BSC 去激活 BTS 相关的有线信道和无线信道。

MS 收到“指配命令”（Assignment Command）消息后，就转到指定的 TCH 信道上。至此 TCH 信道已经建立，无线资源和 A 口资源均已成功分配。

（3）提醒与连接

主叫的 TCH 信道建立成功了，接下来就是等待被叫的响应了。被叫的响应分为两个



过程，第一部分是找到被叫后对被叫进行振铃，称为“提醒”（Alerting）；第二部分是被叫摘机，电话接通，称为“连接”（Connect）。

主叫 MS 收到“提醒”的消息后，说明已经建立了自主叫 MS 至被叫的完整通路。至于被叫是如何找到的，我们不妨放到被叫的信令流程里进行讨论。

当被叫用户摘机以后，被叫端将会向主叫 MSC 发送“应答”（Answer）消息，此时主叫 MS 至被叫 MS 之间的语音话路接通，主叫 MSC 给主叫 MS 发送一条“连接”（Connect）消息，告诉主叫可以进行通话了，主叫 MS 收到该消息后接着就向系统发送一条“连接证实”（Connect ACK）消息，告诉系统可以开始收费了。

至此我们就完成了主叫“搭积木”的所有过程。

8.9 路由，关键就是路由——MS被叫流程

被叫的通话接续过程和主叫基本是一模一样的，收到寻呼消息后就进行随机接入和立即指配，接着就是加密和鉴权，然后就是话音信道的指配。与主叫信令流程不同的是，在通话接续之前我们必须对被叫 MS 进行寻址！

这就是移动通信相对固定通信的一个重要的区别，固定通信被叫的路由是确定的，而移动通信你事先根本就不知道被叫用户的位置，所以路由是不确定的。

8.9.1 被叫的寻址过程

那我们怎么来寻找被叫用户的路由呢？首先得知道哪些伙计都知道被叫MS的位置信息。由于 MS 进行位置更新的缘故，MS 在哪个 MSC/VLR 下 HLR 是知道的，MS 在哪个位置区 VLR 是知道的，通过对 HLR 和 VLR 的查询，我们就知道 MS 大概的区域位置，能建立一条自主叫 MS 至被叫 BSC 的路由。那么 MS 具体在哪个小区谁知道呢？谁都不知道，我们没有法子，只能在整个位置区下发寻人启事，让被叫 MS 主动来接入网络。

我们来勾勒一下路由寻址的大致过程：主叫 MSC/VLR 首先从 HLR 里查询被叫 MS 所在的 MSC/VLR，并建立主叫 MSC/VLR 至被叫 MSC/VLR 的路由；然后从被叫当前所在的 VLR 里查询 MS 所在的位置区；最后在位置区内对 MS 进行寻呼，从而完成最终路由的建立。

我们就以 PLMN 网内的呼叫为例来解释路由的建立，如图 8.33 所示。

（1）MS 用户发起一个呼叫，将被叫 MSISDN（被叫号码）送至 MSC，MSC 经过号码段分析就知道被叫 MS 归属的 HLR，然后就向 HLR 发送路由查询消息，找找被叫 MS 到底跑哪里去了。

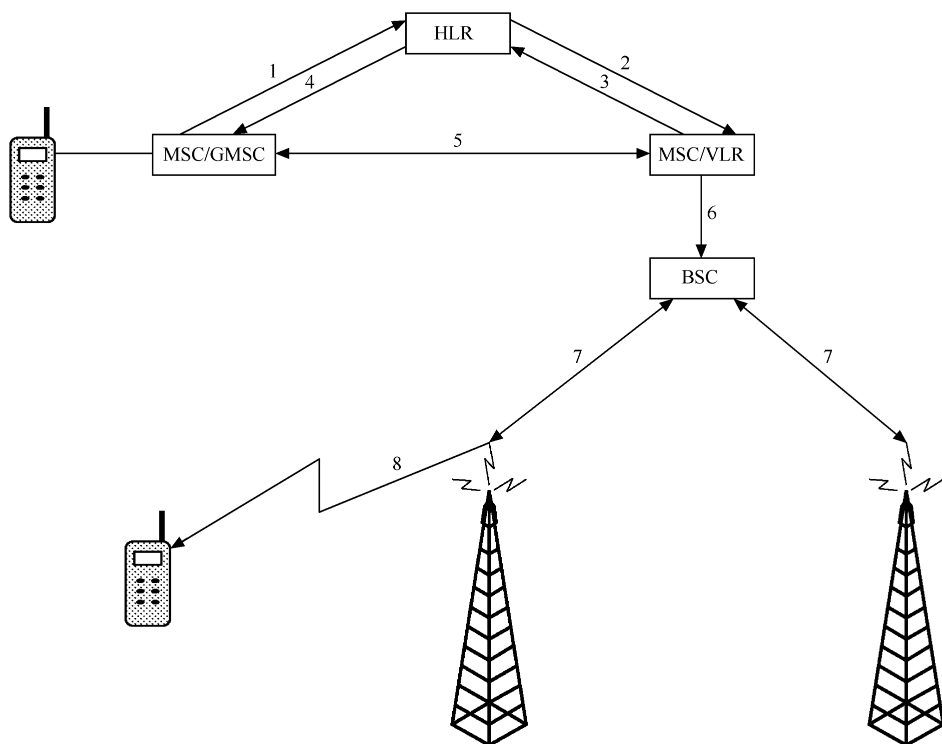


图 8.33　被叫 MS 寻址过程

（2）HLR 里有一张表，表上有 IMSI 和 MSCID 的对应关系，HLR 拿表一比对，就知道 MS 当前所在的 MSC/VLR。那么就向这个 MSC/VLR 发送消息，要求其提供一个漫游号码 MSRN 用于建立路由。

（3）被叫端 MSC/VLR 找到一个空闲的 MSRN，分配给被叫 MS，并将该结果返还给 HLR，该 MSRN 是动态的，呼叫完成后释放掉。

（4）HLR 将漫游号码 MSRN 回送给主叫 MSC。

（5）主叫 MSC/VLR 收到该 MSRN 后，通过 MSRN 可知道被叫端局的地址，然后可以建立端对端的链路。

（6）被叫端 MSC 根据被叫 MS 的 IMSI 号，到 VLR 里查询相关的位置信息，同时将寻呼的相关信息送给 BSC。这个时候漫游号码 MSRN 就没有什么价值了，可以释放了。

（7）BSC 向归属的所有的 BTS 发送寻呼消息。

（8）BTS 根据 TMSI 或者 IMSI，在 PCH 信道上对被叫手机进行寻呼。

MS 响应寻呼后接入网络，被叫的路由完全建立。主叫 MSC/GMSC 和被叫端 MSC/VLR 及 HLR 之间的信令流程如图 8.34 所示。



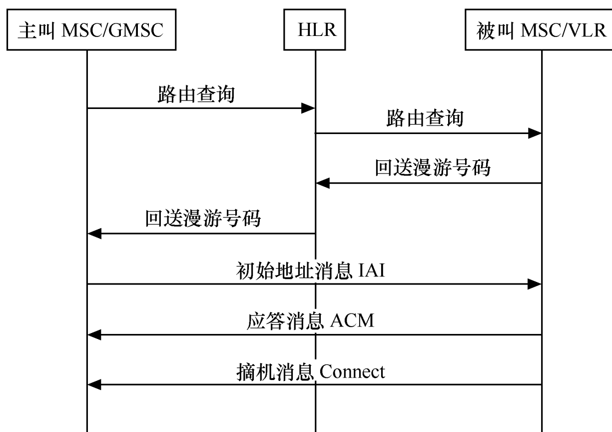


图 8.34　GMSC、HLR、MSC/VLR 之间的信令流程

上面的信令流程列了 8 个步骤，很容易看得人晕头转向，我们稍作休息，来看一个小故事。这个故事叫做**“寻找 A 总”**。

话说 A 总（被叫 MS）是某跨国集团的董事长，找他可不是件容易的事。这天 ITM 公司的小 C（主叫 MS）想找 A 总办理一个业务，但是却被公司（主叫 MSC/VLR）告知 A 总全国各地到处跑，你得先去他总部的行政办公室（HLR）预约。小 C 照办了，就去 HLR 处咨询:“请问 A 总现在在哪里”。HLR 笑而不答，其实 A 总去哪个城市办公室 HLR 都是有记录的，HLR 在系统里一查，发现 A 总现在正在 D 市分公司（被叫 VLR）歇着。HLR 就和 D 市的 VLR 联系：“小 C 要找 A 总，要来你办事处，麻烦行个方便”。D 分公司二话不说，给了 HLR 一张机票（MSRN 号，用于主叫 MS 找到被叫所在的 MSC/VLR），HLR 将这个转给了小 C 的公司，小 C 拿着机票（MSRN 号）就能去 D 市分公司了。这就是路由建立的第一阶段，那就是建立主叫 MSC/VLR 和被叫 MSC/VLR 之间的路由。

小 C 来到了 D 市分公司，听说 A 总正在视察车间（某个位置区 LA），这回他学聪明了，直接跑到 D 市分公司的行政办公室（VLR）咨询 A 总的位置，VLR 告诉他 A 总在 3 号车间。小 C 又跑到 3 号车间，只见车间那么大，人那么多，去找 A 总岂不是大海捞针，他看见车间都装了扩音喇叭，于是灵机一动跑到播音室开始寻人启事:“A 总、A 总，你在哪里，听到请与播音室联系”。等 A 总回应后，那么路由建立的第二阶段也完成了，即建立被叫 MSC/VLR 到被叫 MS 的路由。

路由建立好之后，就可以完成接下来的“提醒”（Alerting）和“连接”（Connect）的流程了。

8.9.2　被叫接续过程

被叫的接续过程和主叫信令流程基本一致，相同的部分不再赘述，在这里我们只说



不同的部分，那就是呼叫建立的原因不同。

作为主叫，建立原因是请求进行呼叫；作为被叫，建立原因是响应寻呼。差别就在寻呼过程，寻呼过程是怎样的呢？

VLR 根据存储的 LAI 地址，向 MSC 发寻呼命令，MSC 收到后会向下属的所有 BTS 发送寻呼消息，BTS 通过 PCH 信道把寻呼消息发送出去，其中包括 MS 的 IMSI/TMSI 号码，MS 在 PCH 信道上收听到自己的寻呼消息后，开始申请信道，原因为响应寻呼，然后在 SDCCH 信道上回送一条寻呼响应（Paging Response）消息。寻呼响应如图 8.35 所示。

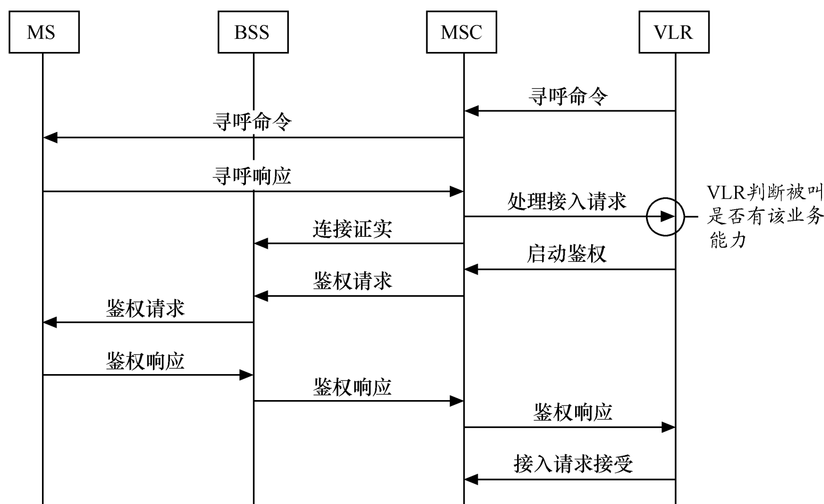


图 8.35　响应寻呼过程

8.10 来试试空中接力——切换原因及流程

切换大概是 GSM 信令流程里最复杂的，要考虑的因素非常多。不仅如此，切换也是 GSM 体系里相当重要的一环，因为此时用户正在通话，你不能因为你的切换过程就让用户掉话。掉话率是运营商考核的很重要的一个指标，掉话是非常影响客户感知的。

切换为什么复杂？我们不妨用足球比赛中的空中接力来形容它，在足球比赛中，几个球员之间连续的空中接力是非常罕见的，因为球不能落地，而要完成这几个动作要考虑的因素是非常之多，来球的方向、高度和力度，队友的跑位情况和速度，对正面防守队员动作的预判，对来球应采取何种方式去踢，垫给队友，脚后跟勾给队友，头球点给队友，亦或脚背搓给队友，种种方式不一而足。球员在一瞬间要根据球场上瞬息万变的形式作出准确的判断，要想连续地接力那是相当得难，正因为如此，空中接力一旦打出



来了，那是相当得漂亮，对手也极难防范。

切换也是件很麻烦的事，空中接力要求球不能落地，切换要求不能出现掉话，而且其要考虑的因素也一点不比空中接力少，首先判断 MS 是否需要切换就是一个复杂的过程，涵盖种种因素：你可能因为手机的 TA 值太大了，嫌距离太远要求切换；你可能因为通信质量太差了要求切换；你可能因为接收电平太低了要求切换，种种不一而足。你确定要切换后，一大堆麻烦事又在等着你，你需要查找哪里有资源，找到资源后又需要对资源进行激活，为了顺利进行切换还需要和邻小区进行同步。这些事情看起来是很麻烦，好在 GSM 系统是由机器组成的，机器干这些机械的活比人可强多了，只要你给它定好规矩和流程，它就能不折不扣地执行。下面就来理一理这些纷繁芜杂的切换过程。

切换，是指将一个正处于呼叫建立状态或通话状态的 MS 转换到新的业务信道上的过程。切换的决定者不是 MS 本身，而是网络。MS 只有对本身信号质量以及接收电平进行测量并上报给网络的权利，至于要不要进行切换，那是网络考虑的事情。就好比一个业务员只有搜集情报上报给部门经理的权力，至于如何进行判断和决策，那是公司层面的事情。

一般情况下，下面的两个原因将导致小区切换的发生。

（1）第一种称之为预防性切换。邻小区提供更好的通信链路，网络层面根据 MS 和 BTS 上报的测量报告进行衡量，觉得邻小区的通信链路质量更好，为了预防起见，就将 MS 进行切换。

（2）第二种称之为紧急切换。若当前的链路质量非常差，或者接收电平很低，或者时间提前量 TA 值太大，都将导致紧急切换。如果没有合适的切换对象，那么就会导致掉话，参见图 8.36。

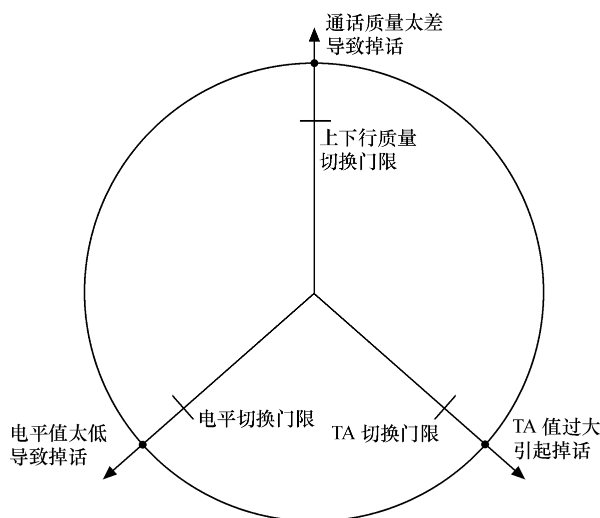


图 8.36　紧急切换条件

我们不妨把接收电平、接收质量和 TA 值看成 GSM 切换的 3 个参数，有一个差得不行了，也就是达到切换值时，我们就需要对其切换。如果在 MS 直到达到释放值了还没有进行切换，那么系统将自动断开 MS 的通话连接，造成一次掉话，如图 8.36 所示。

我们在上面看到了当手机的电平、质量和 TA 值超过一定的值时将引起掉话，所有切换的目的就是为了预防这种情况的发生，那么“切换”究竟是如何完成空中接力，从而避免掉话的产生的呢？我们首先从切换的判决开始说起。

要进行判决，首先得有测量报告。就好比法官要进行判决，先得有证据一样，测量报告从哪里来？从 MS 和 BTS 那里来，它们测量完之后上报给 BSC，BSC 就要进行是否进行切换的考量了，这个过程也称为 Locating（定位），我们来看看图 8.37。

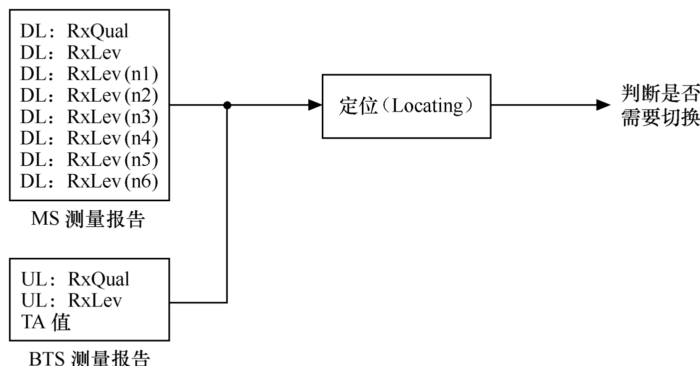


图 8.37　切换判决

从图 8.37 中可以看到，切换判决由两部分组成，其一是测量报告，其二是 Locating。下面首先来了解测量报告是怎么得来的。

8.10.1　测量报告的由来

当 MS 处于通话状态中时，MS 就通过 SACCH 信道收听本小区的系统消息，从而了解所有的邻小区。MS 可以在两个时间段内测量邻小区 BCCH 载频的接收电平：其一是每个 TDMA 帧从收到发这个时间间隙；其二是空闲帧的时候，MS 不仅可以利用空闲帧来测量邻区 BCCH 的电平，还可以利用这段时间来对邻区的 SCH 信道进行解码，从而获得邻区的 TDMA 帧号和 BSIC 码，BSIC 码很重要，可以根据 BCCH 载频的频率和 BSIC 码来确定邻区是否发生了改变（因为原则上是不允许同频同 BSIC 的）。

MS 的测量报告需要 4 个 SACCH 信道才能传送完毕，而在 26 帧的 TCH 复帧中，只有 1 个 SACCH 帧，所以完整上报一份测量报告共需要 480ms（4×4.615ms×26），如图 8.38 所示。



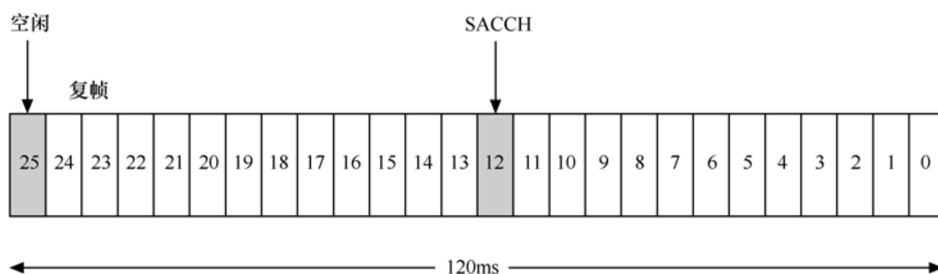


图 8.38　测量报告通过 SACCH 信道传送

Locating 所需的数据需要 MS 对下行链路（DL）进行测量，包括本小区的接收电平和接收质量，以及 6 个邻小区的接收电平，然后通过 SACCH 信道发送给 BTS，如图 8.39 所示。

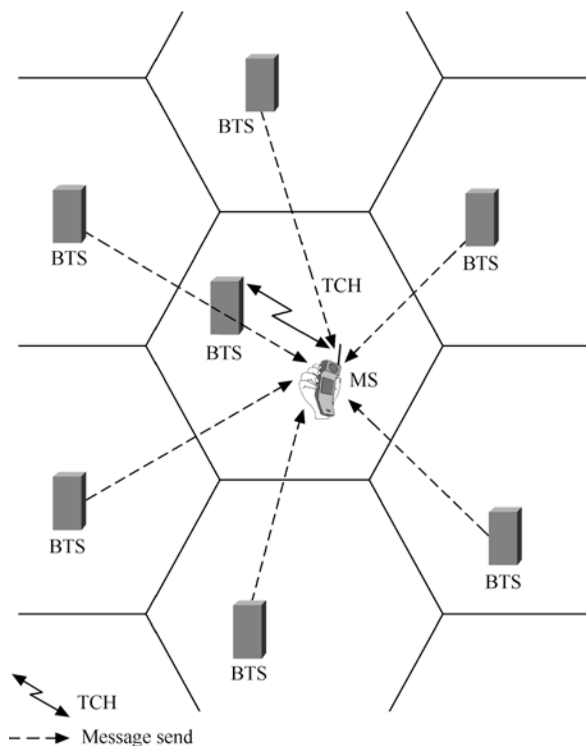


图 8.39　MS 测量当前小区及邻小区的数据

除了 MS，BTS 也需要进行测量，它测量的是 MS 的上行链路（UpLink）。BTS 的测量报告中包括了上行链路的信号强度和信号质量，以及 TA 值。

因此一份完整的测量报告说明了当前服务小区上下行链路的信号强度以及信号质量，TA 值，6 个邻小区的接收电平、载频号和 BSIC 值，以及与 RRM 有关的 DTX 使用指示和功率等级。

信号的强度是用 dBm 来衡量的，从−47～−110dBm，对应数值的 0～63；信号的质量使用误比特率（BER）来衡量，RxQual 测量值范围为 0～7。

下面我们来看看 RxLev 和 RxQual 的参数对应表，见表 8.8 和表 8.9。

表 8.8 信号强度的参数范围

信 号 强 度	参 数 范 围
RxLev 0	<−110dBm
RxLev 1	−110～−109dBm
RxLev 2	−109～−108dBm
⋮	⋮
RxLev 61	−50～−49dBm
RxLev 62	−49～−48dBm
RxLev 63	>−48dBm

表 8.9 话音质量等级

质 量 等 级	误 码 率	假 定 值
RxQual 0	<0.2%	0.14%
RxQual 1	0.2%～0.4%	0.28%
RxQual 2	0.4%～0.8%	0.57%
RxQual 3	0.8%～1.6%	1.13%
RxQual 4	1.6%～3.2%	2.26%
RxQual 5	3.2%～6.4%	4.53%
RxQual 6	6.4%～12.8%	9.05%
RxQual 7	>12.8%	18.1%

8.10.2 切换考虑的因素

测量报告说完了，下面我们来谈谈 Locating。GSM 规范里并没有给出 Locating 的严格定义，只是给出了一些参考建议，所以各个厂家往往都有自己的实现方法。我们在这里列举一下哪些情况会导致切换。



1. 预防性功率预算切换

我们希望移动用户的通话永远建立在电平最高的小区上，尤其当移动台穿越两小区的边界时，如果 BSC 根据移动台的测量报告发现邻小区的接收电平满足一定的要求时，就将触发该小区的功率预算切换。这是最常见的一类切换，一般占 50%左右，这类切换的特点叫做提前准备，有备则无患，很符合电信业注重通信保障的特性。其公式如下：

$$PBGT(n) - HoMargin(n) > 0$$

其中

$$PBGT(n) = RxLev_Ncell(n) - [RxLev_DL + nPb] + Pa$$

$$nPb = BsTxPwrMax - BsCurrentTxPwr$$

$$Pa = \mathrm{Min}(MsTxPwrMax, MsTxPwr) - \mathrm{Min}(MsTxPwrMaxCell(n), MsTxPwr)$$

式中，$RxLev_Ncell(n)$为移动台测得的其邻小区的接收电平，单位为 dBm；$RxLev_DL$ 为移动台测得的服务小区的下行接收电平，单位为 dBm；$BsTxPwrMax$ 为基站的最大允许发射功率，单位为 dBm；$BsCurrentTxPwr$ 为基站当前的发射功率，单位为 dBm；$MsTxPwrMax$ 为移动台的额定最大发射功率，单位为 dBm。

应当说上面这个公式所包含的参数很多，非常难以理解，那我们就来一级级分解了看。假设你来设计一个参数 $PBGT(n)$，你会怎样做？

首先我肯定是考虑邻小区的接收电平比当前小区到底要高多少，这样就可以得出公式为：$PBGT(n) = RxLev_Ncell(n) - RxLev_DL$。我们得记得，手机与网络通信时通常是有功率控制的，下行电平不够强，可能是因为功率控制所制，下一秒就能增大发射功率，从而使接收电平增强。我们需要考虑功率控制的因素，那么下行电平还有多少可以增加的空间自然也成为需要衡量的因素，这个因素用 nPb 来表示。那么 $PBGT(n)$ 的表达式就变成了：

$$PBGT(n) = RxLev_Ncell(n) - [RxLev_DL + nPb]$$

我们刚刚考虑的都是下行，但通信不止有下行，还有上行。在上行方向我们希望这条信道的发射功率越小越好，以避免干扰系统里其他的 MS。对于这个愿望，我们用 Pa 来表示，以在上行信道可以发射的最大功率为准绳，发射功率越小我们越喜欢。综合考虑上行的因素，那么 $PBGT(n)$ 的表达式就变成了：

$$PBGT(n) = RxLev_Ncell(n) - [RxLev_DL + nPb] + Pa$$

满足该公式且 $PBGT(n)$ 最大的邻小区将被选为切换的目标小区。在这里面有一个切换容限（HoMargin）的概念，它也是在邻小区切换参数中定义的。GSM 把它引入的目的是为了增加切换的难度，来预防当服务小区的接收电平和其邻小区的接收电平差不多时所引起的乒乓效应，即在两小区之间来回地频繁切换。但该值又不能设置过高，以



防引起切换不过去而导致掉话现象的发生。

2. 救援性电平切换

在小区切换参数里定义了上下行电平切换门限值，当 BSC 从移动台和基站的上（下）行测量报告中发现上（下）行接收电平值低于参数所定义的上（下）行电平切换门限值（该值应比小区的最小接入电平高），它将从测量报告中选择一个合适的邻小区来进行切换，如果没有合适的邻小区，那么很容易导致掉话的发生。

在这种类型的切换过程中，其邻小区的接收电平应满足比服务小区的高出一定的值，该值被称为救援性电平切换容限（*HoMargin_RxLev*），其目的也是为了避免引起乒乓切换。在郊区基站比较少，就应该降低该值以使救援切换及时发生；而在基站密集的地方，则应该提高该值，以避免乒乓切换。由于救援性电平切换是发生在本小区的接收电平已经很差的情况下，因此其切换容限应该低于功率预算切换，以便救援性电平切换可以被触发。

3. 救援性质量切换

原理同上，当通话质量差得超过门限值，就触发该种切换。

针对该种切换，也有一个救援性质量切换容限（*HoMargin_RxQual*），对该值设置应该要宽松一些。只要目标小区的信号电平不比当前小区差很多，就应该鼓励切换，以尽量改善正在进行通话的质量。

4. TA 值引发的切换

该项切换的目的是为了控制基站的覆盖范围，减小系统的干扰。当 BSC 发现 MS 汇报的 TA 值超过门限时，就引发切换，如图 8.40 所示。

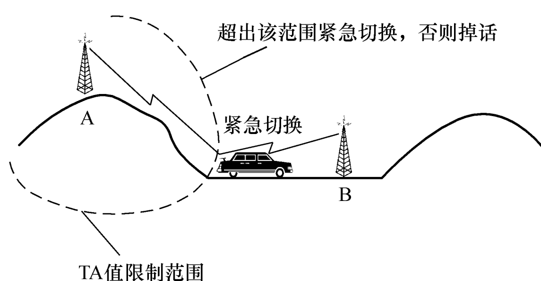


图 8.40　TA 值规定的覆盖范围

5. 话务切换

在呼叫建立阶段，小区首先会分配 SDCCH 以连通移动台和基站，并进一步分配话音信道 TCH 以建立通话信道，若此时该服务小区无空闲的 TCH，通常会导致因 TCH 的拥塞而试呼失败。为了充分利用周围的无线资源以减少拥塞，系统提供了话务切换功能。此时 SDCCH 已经指配成功，而该小区却无空闲的 TCH 信道，则 BSC 将根据移动台的测量报告来指示将通话接入到最佳邻小区的空闲话音信道上来。



8.10.3　切换的信令流程

根据测量报告，BSC 作出了决策，决定要不要进行切换。如果一旦决定要进行切换，那么信令流程又是怎样的呢。我们接着进行讨论。

按照切换点的不同，可以分为小区内切换、BSC 内切换、MSC 内切换和 MSC 之间的切换。

1. 小区内的切换

小区内部的切换和 TCH 信道指配比较相似，就不再讨论。

2. BSC 内的切换

同一 BSC 的切换是发生得最多的切换，我们也希望减少跨 BSC 的切换，以降低信令负荷。具体流程（见图 8.41）如下：

（1）BSC 根据定位（Locating）决定要进行切换，然后向新小区发送“信道激活”（Channel Activation）消息，要求提供一条 TCH 信道准备接收切换。新小区准备好以后，那么将向 BSC 返回一条“信道激活证实”（Channel Activation ACK）消息。

（2）BSC 通过 FACCH 信道向旧 BTS 发送“切换命令”（Handover Command）消息，包括新信道的频率、时隙和信道最大发射功率等参数，BTS 将该命令下发 MS。

（3）MS 把频率调谐至新的频率上，然后通过 FACCH 信道向新小区发送一个切换接入突发脉冲。

（4）新 BTS 收到此突发脉冲后，一方面向 BSC 发送“切换检测到”（HO Detect）消息，另一方面通过“物理消息”（Physical Information）将时间提前量信息通过 FACCH 回送给 MS。

（5）MS 在新的 TCH 信道上发送 SABM 帧用来建立数据链路层的连接，BTS 收到该消息，一面向 BSC 发送“建立指示”（Establish Indication）说明数据链路层已经建立，一面向移动台发送 UA 帧用于证实。

（6）移动台收到 UA 帧后，就认为连接已经完全建立，然后通过新 BTS 向 BSC 发送“切换成功”（Handover Complete）消息。

（7）BSC 要求旧 BTS 释放 TCH 信道。

（8）整个过程不需要 MSC 参与，切换完成后 BSC 会向 MSC 发送一条“切换完成”消息。

心理学家说，人瞬间记忆的数字很难超过 7 个；管理学家说，一个管理者直接管理的下属最好不要超过 8 个，这是一般人能做到的极限。这切换的信令流程冲上来就列举



了 8 个步骤，一时之间还真是难让人很快消化。我们把它抛开一边，稍作休息，先看一个“**MS 换销售区域**”的故事。

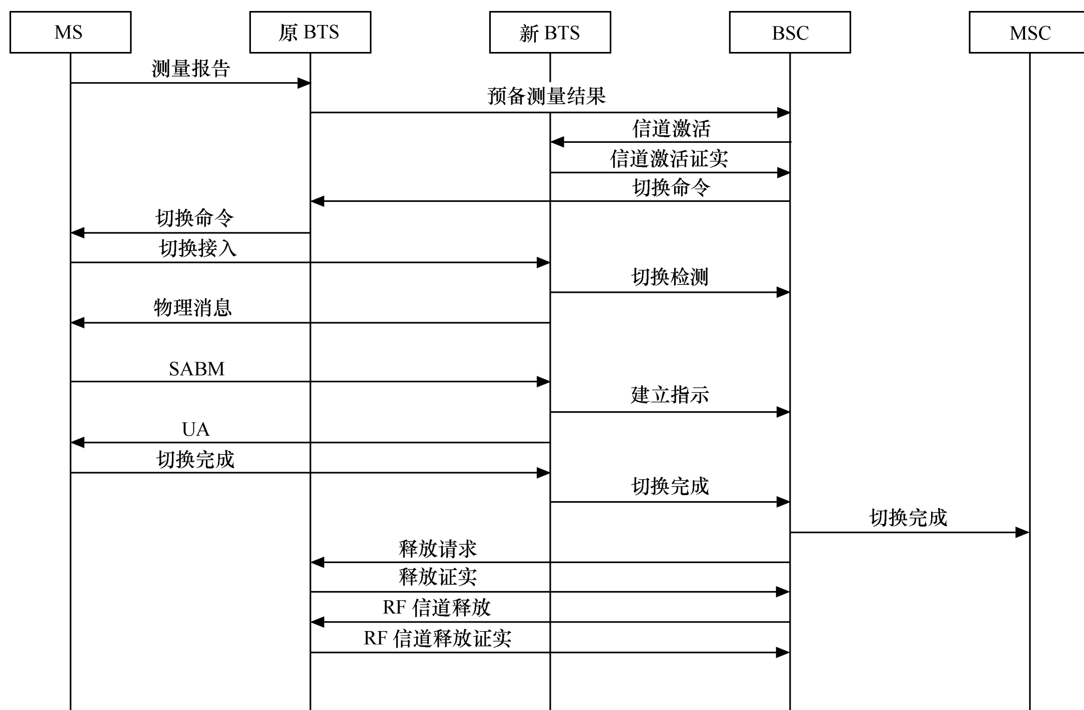


图 8.41　BSC 小区内切换信令流程

MS 是 ITM 公司一个非常优秀的销售代表，但是这些天他与他的直接主管 BTSA 之间有点不愉快。ITM 公司有这样的制度，销售代表和销售主管之间都要定期进行业绩互评（测量报告）并上交销售经理，好让销售经理对全盘有个掌控。业绩互评主要包括以下内容：销售代表评价销售主管的支持力度和支持效果（MS 测量 BTS 的下行电平和下行通信质量），销售主管评价销售代表的销售力度和销售效果（BTS 测量 MS 的上行电平和上行通信质量），销售代表对销售主管的评价也通过销售主管转交给销售经理 BSC，但是销售主管只负责转交，不能对报告进行任何处理（BTS 透明传输测量报告）。

BSC 发现近段 MS 对 BTSA 的评价越来越差，BTSA 对 MS 的评价也好不到哪里去（可能是因为 MS 正在远离 BTSA 或者因为干扰问题导致通信质量变差）。BSC 眉头紧皱，通过 Locating 程序一算，就决定把 MS 从 BTSA 的管辖范围调离，调到 BTSB 手下。不过在此之前他先得咨询一下 BTSB 的想法，毕竟强扭的瓜不甜。于是他就试探性地问 BTSB：“你那里 × × 销售岗位还有空缺没，MS 想过来。”（BSC 向新 BTS 发送“信道激



活”消息），BTSB 觉得自己这里还容得下一个人，于是就向 BSC 报告：“俺这里还有地方。”（新 BTS 向 BSC 发送“信道激活证实”消息）

BSC 现在心中有数了，就通知 MS 原来的主管 BTSA：“MS 从后天起到 BTSB 处上班，麻烦转告一下。”BTSA 把这个消息转告给了 MS（BSC 向旧 BTS 发送“切换命令”，BTS 将该消息转给 MS）。MS 大喜，就调整好自己的状态，到 BTSB 的区域报到（MS 调谐到 BSC 指定的频率上，向 BTSB 发送“切换接入突发脉冲”）。BTSB 一边向上级 BSC 汇报 MS 已经来我们区域报到了（新 BTS 向 BSC 发送“切换检测到”消息），一边告诉 MS 我知道你来了以及一些注意事项（新 BTS 向 MS 发送“物理消息”）。

这时候并不代表一切就绪了，MS 需要搞清楚注意事项（比如时间提前量），然后通知 BTSB 我已经准备好了，可以进入工作状态了（MS 向新 BTS 发送 SABM 帧，用于建立数据链路层）。BTSB 一边向 MS 点头表示对他如此快进入工作状态表示赞许（新 BTS 向 MS 发送 UA 帧用于证实），一边向 BSC 表示 MS 已经融入团队了（新 BTS 向 BSC 发送“建立指示”说明新 BTS 和 MS 的数据链路层已经建立）。MS 收到 BTSB 的 UA 帧赞许后，就通过 BTSB 向 BSC 汇报说转换区域已经成功（MS 通过新 BTS 向 BSC 发送“切换成功”消息）。

3. 相同 MSC 下不同 BSC 之间的切换

这种切换需要 MSC 和两个 BSC 共同参与控制，呼叫完成后 MS 还须进行位置更新，如图 8.42 所示，其信令流程如下：

（1）旧 BSC 根据测量报告，把切换请求及切换目的小区标识一起发给 MSC。

（2）MSC 判断是哪个 BSC 控制的 BTS，并向新 BSC 发起切换请求。

（3）新 BSC 要求 BTS 激活一个 TCH 信道。

（4）新 BSC 把包含有频率、时隙及信道最大发射功率的信息通过 MSC、旧 BSC 和旧 BTS 传到 MS。

（5）MS 把频率调谐至新的频率上，然后通过 FACCH 信道向新小区发送一个切换接入突发脉冲。

（6）新 BTS 收到此突发脉冲后，一方面向新 BSC 发送“切换检测到”（HO Detect）消息，另一方面通过“物理消息”（Physical Information）将时间提前量信息通过 FACCH 回送给 MS。

（7）移动台收到 UA 帧后，就认为连接已经完全建立，然后通过新 BTS 向新 BSC 发送“切换成功”（Handover Complete）消息。

（8）MSC 命令旧 BSC 去释放 TCH，旧 BSC 命令旧 BTS 执行。

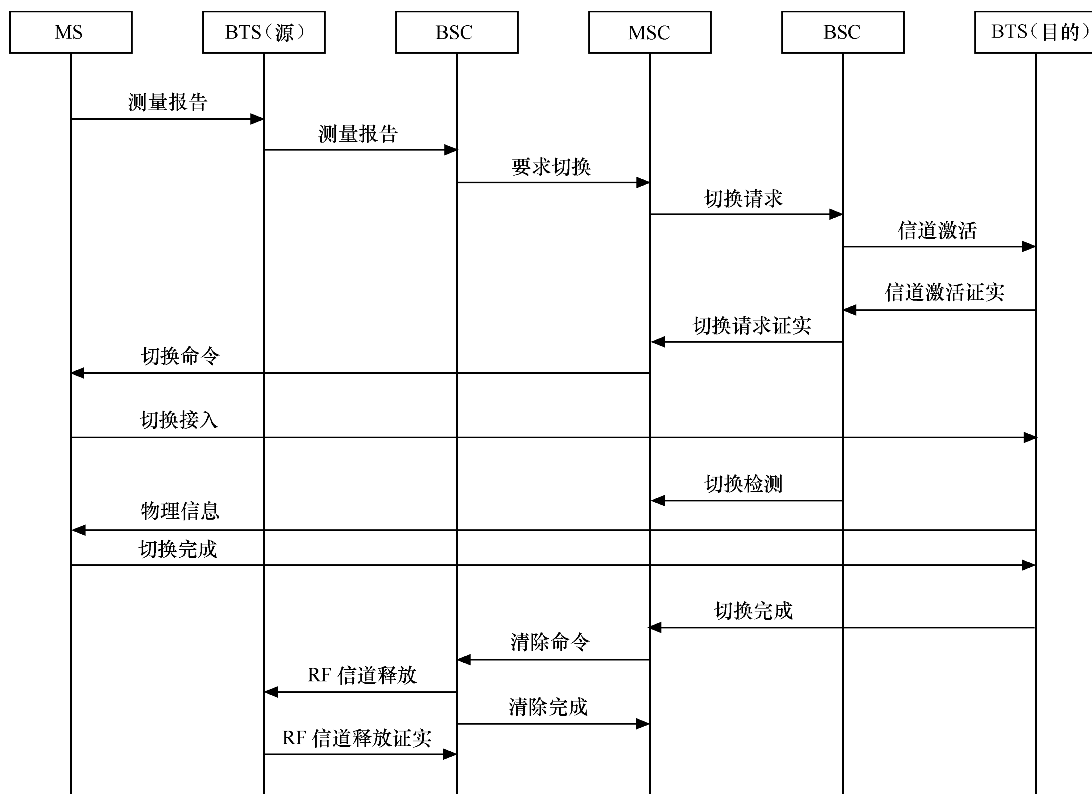


图 8.42　MSC 内部切换

我们可以看到，相同 MSC 不同 BSC 的切换相比 BSC 内部的切换，信令流程中唯一不同的地方在于原来一个 BSC 完成的工作现在由两个 BSC 在完成。内容相差不大，大家可以参考一下第 2 点，就不再展开论述。

4．不同 MSC 之间的切换

这是最复杂的一种情况，涉及两个 MSC，我们称切换前 MS 所处的 MSC 为 MSC_A，切换后 MS 所处的 MSC 为 MSC_B。我们来看看它的信令流程，如图 8.43 所示。

（1）旧 BSC 根据测量报告进行 Locating 计算之后，发现切换的目标小区不属于该 BSC，就向 MSC 发送一条切换请求消息。

（2）MSC_A 判断出小区属另一个 MSC 管辖，然后通过 MAP 协议发送“切换准备”消息与 MSC_B 建立联系。

（3）MSC_B 收到 MSC_A 的切换请求后，就发送“分配切换号码”消息给 VLR_B。VLR_B 通过“发送切换报告”消息将切换号码告诉 MSC_B。切换号码的分配只是为了



使归属 MSC_A 能够建立起来与目标 MSC_B 之间的路由而提供的一个指向。

（4）MSC_B 向 BSC_B 发出“切换请求”，由 BSC_B 将目标小区的信道激活。

（5）MSC_B 收到 BSC_B 的回送信息并将切换号（HO Number）在“切换准备证实”消息中一起传送给 MSC_A。

（6）MSC_A 通过 BSC_A 向 MS 发送切换命令，包括频率、时隙和最大发射功率。

（7）MS 通过 FACCH 信道在新频率上发送以接入突发脉冲。

（8）BTS_B 收到申请后，通过 FACCH 回送时间提前量。

（9）MS 通过 MSC_B 和 MSC 发送“切换成功”消息，随后旧的 TCH 信道被释放。

由于是跨 MSC 切换，通话完毕后需要做位置更新。

MS
BSC_A
MSC_A
MSC_B
BSC_B
VLR_B
测量结果
要求切换
切换准备
分配切换号码
发送切换报告
切换请求
切换请求证实
切换准备证实
IAI (HO Number)
ACM
切换命令
切换完成
清除命令
清除完成

图 8.43　不同 MSC 之间的切换

应当说第 4 点和第 3 点之间差别也不是很大，只是多了一个 MSC_A 和 MSC_B 之间寻址和建立路由的环节，其余内容大同小异。

8.11 本章小结

对于一个实际的商用无线通信网络而言，信令流程是最为重要的一环。为什么说它重要呢？因为它定义了一个网络的运作机制，它必须严谨、有效、环环相扣，才能保证一个庞大而又复杂的系统有条不紊地运行。

所谓“流程”，你不妨把它看作流水作业；所谓“信令”，你不妨把它看作流水线上每道步骤的指令。如果你对一个产品途经流水线每个步骤要做的动作都了然于胸，你自然会对这个产品有比较全面和深入的了解。熟悉了信令流程，你就会对信号的走向和网络设备的运转有一个系统的认识。这是信令流程对于理解无线通信网络而言一个方面的价值。

同时，熟悉信令流程还非常有利于对网络进行分析和排障。这也很好理解。如果你对一条流水线都很熟悉的话，那么一个产品出了问题，你经过分析，自然就知道应该去哪个环节进行排障。如果你对整个信号的流程熟悉了的话，那么碰到一些疑难杂症，比如说掉话，你就不会束手无策，而是会去进行信令跟踪，然后到你脑海中的那幅“信号流程图”里按图索骥。是接收电平的问题？还是切换的问题？亦或是拥塞？把一个呼叫进行一下信令跟踪，一切亦然明了。

最后再强调一下，信令流程是通信网络中极复杂也是极重要的一环，希望大家要重点掌握。

参 考 文 献

[1] （美）ALAN V.Oppenheim 著．信号与系统（第 2 版）．刘树棠译．西安：西安交通大学出版社，1998．

[2] （美）Charles Petzold 著．编码的奥秘．伍卫国，王宣政，孙燕妮等译．北京：机械工业出版社，2004．

[3] （印）Atul Kahate 著．密码学与网络安全．邱仲潘等译．北京：清华大学出版社，2005．

[4] 樊昌信等．通信原理（第 5 版）．北京：国防工业出版社，2005．

[5] （美）John G.Prokis，Masoud Salehi 著．通信系统原理．李锵，关欣，杨爱萍，董健译．北京：电子工业出版社，2006．

[6] （美）Theodore S.Rappport 著．无线通信原理与应用．周文安，付秀花，王志辉等译．北京：电子工业出版社，2006．

[7] （美）William C.Y.Lee 著．无线与蜂窝通信．陈威兵，黄晋军，张聪译．北京：清华大学出版社，2008．

[8] （美）William Stallings 著．无线通信与网络．何军等译．北京：清华大学出版社，2005．

[9] （美）David Tse 等著．无线通信基础．李锵等译．北京：人民邮电出版社，2007．

[10]（美）Andrea Goldsmith 等著．无线通信．杨鸿文等译．北京：人民邮电出版社，2007．

[11] 张威．GSM 网络优化——原理与工程．北京：人民邮电出版社，2003．

[12] 韩斌杰，杜新颜，张建斌．GSM 原理及其网络优化（第 2 版）．北京：机械工业出版社，2009．

[13] 孙宇桐，赵文伟，蒋文辉．CDMA 空中接口技术．北京：人民邮电出版社，2004．

[14] （芬）Harri Holma，Antti Toskala 著．WCDMA 技术与系统设计：第三代移动通信系统的无线接入（原书第 3 版）．陈泽强等译．北京：机械工业出版社，2005．

[15] 孙儒石等．GSM 数字移动通信工程．北京：人民邮电出版社，1998．

[16] 叶敏．程控数字交换与交换网．北京：北京邮电大学出版社，2003．

[17] （美）William Stallings 著．计算机组织与体系结构．张昆藏等译．北京：清华大学出版社，2005．

[18] （美）James F.Kurose，Keith W.Ross 著．计算机网络自顶向下方法（原书第 4 版）．陈鸣译．北京：机械工业出版社，2009．

[19] 纪红．7 号信令系统（修订本）．北京：人民邮电出版社，1999．



[20] YD/T855.21-1996．900MHZ TDMA 数字蜂窝移动通信网无线接口信令部分

[21] YD/T855.22-1996．900MHZ TDMA 数字蜂窝移动通信网无线接口物理层部分

[22] 摩托罗拉工程学院．MCNE-CP02：GSM 数字蜂窝概述

[23] 摩托罗拉工程学院．MCNE-BSS11：BSS 工作原理

[24] 摩托罗拉工程学院．MCNE-BSS08：BSSC 应用

[25] 摩托罗拉工程学院．MCNE-SYS01：GSM 接口和协议

[26] 摩托罗拉工程学院．MCNE-SYS02：BSS 数据库概述

[27] http://americanhistory.about.com

[28] 张中荃．程控交换与宽带交换．北京：人民邮电出版社，2003．

[29] 华为技术有限公司．七号信令视频教程

[30] 中国科普网. http://zlg.kepu.gov.cn

[31] 中国业务无线电. http://www.hellocq.com

[32] 赛迪网数码消费类电子产品频道.http://ezit.ccidnet.com

[33] 中国电信集团公司. http://www.chinatelecom.com.cn